JUSTITSMINISTERIET

Databeskyttelsesforordningen

– og de retlige rammer for dansk lovgivning

Betænkning nr. 1565

Del I – bind 1

Betænkning om

Databeskyttelsesforordningen (2016/679)

– og de retlige rammer for dansk lovgivning

Del I, bind 1

Betænkning nr. 1565

Databeskyttelsesforordningen

Betænkning nr. 1565

Publikationen kan bestilles via Justitsministeriets hjemmeside (www.justitsministeriet.dk)

eller hos

Rosendahls Lager og Logistik
Vandtårnsvej 83A
2860 Søborg
Telefon 43 22 73 00
distribution@rosendahls.dk
http://jm.schultzboghandel.dk

ISBN: 978-87-93469-10-5
ISBN internet: 978-87-93469-11-5

Tryk: Rosendahls a/s

Pris: 300 kr. incl. moms

Indholdsfortegnelse

Del I: Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning

1. Indledning

1.1. Den generelle EU-forordning om databeskyttelse

I januar 2012 fremsatte EU-Kommissionen forslag til en databeskyttelsespakke. Pakken blev endeligt vedtaget den 14. april 2016.

Pakken består navnlig af den generelle forordning nr. 2016/679 om beskyttelse af personoplysninger, som skal gælde i både den private og offentlige sektor (databeskyttelsesforordningen). Forordningen anvendes fra den 25. maj 2018. Herudover består databeskyttelsespakken af et direktiv om beskyttelse af personoplysninger, som skal gælde for retshåndhævelsesområdet (retshåndhævelsesdirektivet). Retshåndhævelsesdirektivet er gennemført i dansk ret ved lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger.

Databeskyttelsesforordningen afløser databeskyttelsesdirektivet[1], som i dansk ret er gennemført ved persondataloven, jf. lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.

Databeskyttelsesforordningen fastslår, at databeskyttelse er en grundlæggende rettighed efter EU's Charter om grundlæggende rettigheder og traktaten om Den Europæiske Unions funktionsmåde (TEUF). Som det nævnes i forordningens præambel, har den hastige teknologiske udvikling og globaliseringen skabt nye udfordringer, hvad angår beskyttelse af personoplysninger. Denne udvikling kræver en stærk og mere sammenhængende databeskyttelsesramme i EU, som understøttes af effektiv håndhævelse, for at skabe den tillid, der gør det muligt, at den digitale økonomi kan udvikle sig på det indre marked.

1.2. Justitsministeriets projektarbejde om indretning af dansk lovgivning efter databeskyttelsesforordningen

Databeskyttelsespakken blev som nævnt vedtaget den 14. april 2016, og Danmark havde således fra denne dato ca. 2 år til at tilpasse dansk lovgivning til reglerne i forordningen.

Som følge af denne relativt korte tidsramme for tilpasning af dansk lovgivning til forordningen, igangsatte Justitsministeriet et hurtigtarbejdende projektarbejde, som skulle danne grundlag for arbejdet med at tilpasse dansk lovgivning til forordningen.

Justitsministeriet vurderede således, at det på grund af den korte tidsramme ikke var muligt at tilpasse dansk lovgivning til forordningen ved et traditionelt udvalgsarbejde.

[1] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Justitsministeriet vurderede endvidere, at projektarbejdets analyser burde være afsluttet senest i maj 2017, idet det er hensigten, at de nødvendige lovforslag vil blive fremsat i Folketinget i efteråret 2017, således at der er tid til eventuelle tilpasninger af procedurer hos private virksomheder og myndigheder mv.

Som resultat af projektet med at tilpasse dansk lovgivning til forordningen, besluttede Justitsministeriet, at der bl.a. skulle udarbejdes en betænkning med de nærmere analyser af forordningens bestemmelser, herunder forordningens rammer for nationale særregler og en analyse af konsekvenserne for gældende dansk lovgivning. Endvidere skulle forordningens nye særlige krav hurtigt beskrives og afklares med henblik på vejledning.

I forbindelse med analyserne er der i vidt omfang taget stilling til, om og i givet fald hvordan der inden for rammerne af forordningen kan og skal opretholdes og fastsættes særlige danske regler.

Projektets formål var således overordnet at sikre, at dansk lovgivning kunne indrettes i overensstemmelse med forordningens bestemmelser med virkning fra den 25. maj 2018.

Projektarbejdets analyser er sammenstillet i denne betænkning.

1.3. Organiseringen af projektarbejdet med databeskyttelsesforordningen

Justitsministeriet har siden sommeren 2016 i samarbejde med samtlige ministerier, KL og Danske Regioner samt Erhvervsstyrelsen, Digitaliseringsstyrelsen og Datatilsynet foretaget et analysearbejde af forordningen.

Dette analysearbejde har foregået i et projekt med en styregruppe og projektgrupper, som har stået for arbejdet med databeskyttelsesforordningen.

Arbejdet i projektgrupperne har været understøttet af en række arbejdsgrupper og en ekspertreferencegruppe.

Styregruppen

Styregruppen har overordnet været ansvarlig for projektets gennemførelse og bestod af afdelingschef for Justitsministeriets lovafdeling Jens Teilberg Søndergaard, Datatilsynets direktør Cristina Angela Gulisano, Digitaliseringsstyrelsens direktør Lars Frelle-Petersen og Erhvervsstyrelsens direktør Betina Hagerup.

Projektgrupperne
Projektet har været opdelt i to projektgrupper, hvoraf den ene arbejdede med forordningens rammer for nationale særregler. Den anden gruppe arbejdede – bl.a. med bidrag fra den første projektgruppe – med forordningens konsekvenser for den generelle databeskyttelseslovgivning i Danmark.

Projektgrupperne har været sammensat af medarbejdere fra Justitsministeriet, Datatilsynet, Digitaliseringsstyrelsen, Erhvervsstyrelsen, Erhvervsministeriet, Skatteministeriet, Sundheds- og Ældreministeriet, Danske Regioner og KL. Arbejdet i projektgrupperne har været understøttet af en række arbejdsgrupper.

Arbejdsgrupperne
Den projektgruppe, der behandlede spørgsmålet om rammerne for nationale særregler, har været understøttet af to arbejdsgrupper, mens projektgruppen, der arbejdede med forordningens konsekvenser for den generelle databeskyttelseslovgivning, har været understøttet af fem arbejdsgrupper inddelt efter forordningens forskellige elementer (behandlingsregler og rettigheder, behandlingssikkerhed, nye særlige krav, erstatning og straf samt tilsyn).

Arbejdsgrupperne har været sammensat af medarbejdere fra Justitsministeriet, Datatilsynet, Digitaliseringsstyrelsen, Erhvervsministeriet, samt i det omfang andre ministerier, kommunerne (KL) og regionerne (Danske Regioner) vurderede det relevant, medarbejdere/repræsentanter herfra.

Ekspertreferencegruppen
Arbejdet i projektgrupperne har været understøttet af en ekspertreferencegruppe bestående af kommitteret ved Folketingets Ombudsmand Jens Møller, professor, dr.jur. Peter Blume, professor, dr.jur. Henrik Udsen og ph.d. Gert Læssøe Mikkelsen. En lang række centrale afsnit i betænkningen er efter godkendelse i projektgrupperne blevet forelagt ekspertreferencegruppen. Ekspertreferencegruppen har således været inddraget i centrale afsnit i betænkningens første del vedrørende forordningens kapitel 1-4 og 6-9. Der er i analysearbejdet taget højde for ekspertreferencegruppens bemærkninger, som er indarbejdet i betænkningen.

Herudover blev der i forbindelse med projektarbejdet afholdt "stormøder", hvor bl.a. interesseorganisationer, erhvervslivet og advokatkontorer med speciale i persondataret var repræsenteret.

I efteråret 2016 blev der afholdt et workshop-forløb i regi af Erhvervsstyrelsen, hvor erhvervslivet havde identificeret centrale problemstillinger for erhvervslivet vedrørende forordningen. I forlængelse heraf afholdt Justitsministeriet i samarbejde med Erhvervsstyrelsen et stormøde med deltagere fra erhvervslivet, hvor foreløbige konklusioner om centrale problemstillinger blev præsenteret. Til stormøderne blev der endvidere stillet en række konkrete spørgsmål, som efterfølgende er indgået i analysearbejdet.

I efteråret 2016 blev der endvidere afholdt en række netværksmøder for offentlige myndigheder i regi af Digitaliseringsstyrelsen, hvor offentlige myndigheder havde identificeret centrale problemstillinger for myndigheder vedrørende forordningen. I forlængelse heraf afholdt Justitsministeriet i samarbejde med Digitaliseringsstyrelsen et netværksmøde, hvor spørgsmål om centrale problemstillinger blev besvaret.

Justitsministeriet har i forbindelse med analysearbejdet deltaget aktivt i den af Kommissionen nedsatte ekspertgruppe om databeskyttelsesforordningen, bestående af EU-Kommissionen og de 28 medlemslande, hvor "knaster" i forordningen i forbindelse med gennemførelsen løbende bliver drøftet.

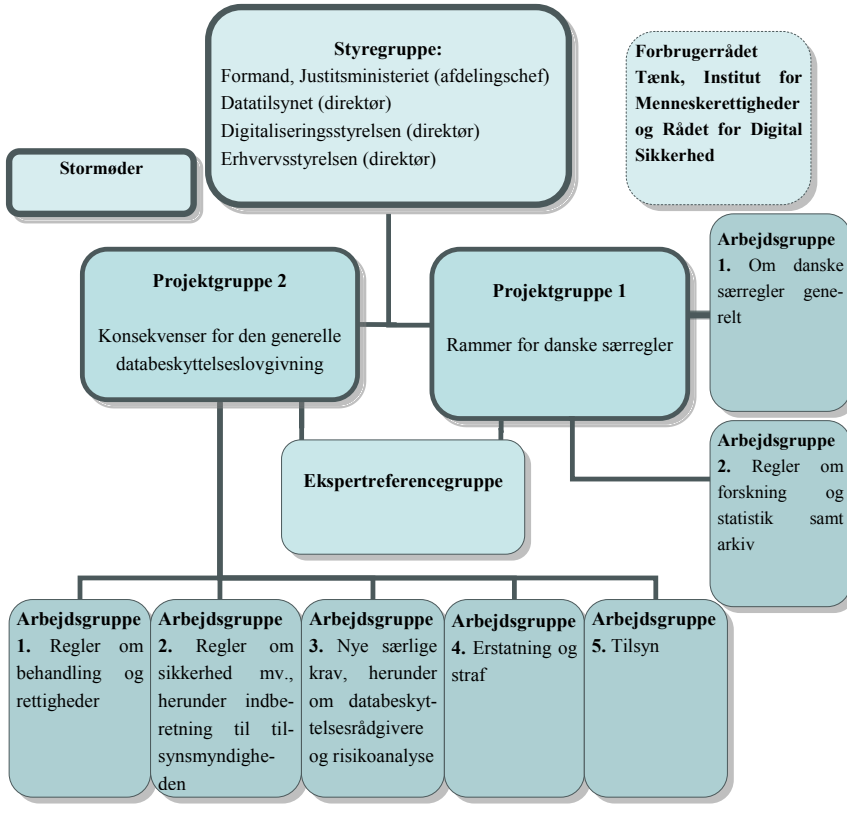
Justitsministeriet har prioriteret dette arbejde højt med henblik på at varetage danske interesser i forbindelse med fortolkningen af forordningen.

Justitsministeriet har i forbindelse med analysearbejdet endvidere deltaget i en række møder med "like-mindede" lande, hvor den nationale gennemførelse af forordningen er blevet drøftet. Disse lande har været Tyskland, Holland, Sverige, Finland, Luxembourg og Irland.

Endvidere har der i forbindelse med arbejdet været særskilte drøftelser om en lang række centrale artikler i databeskyttelsesforordningen med bl.a. Forbrugerrådet Tænk, Institut for Menneskerettigheder og Rådet for Digital Sikkerhed. Der har også i forbindelse med arbejdet været løbende drøftelser med arbejdsmarkedets parter.

I løbet af analysearbejdet har Justitsministeriet endvidere modtaget henvendelser fra en række organisationer, institutioner mv. Dette gælder bl.a. Dansk Erhverv, Dansk Industri, Indsamlingsorganisationernes Brancheorganisation, Forsikring og Pension, Danske Advokater, FSR, Finansrådet, Danske Medier, ATP og en række forsyningsselskaber, som er indgået i analysearbejdet.

Illustration af projektarbejdet:



1.4. Betænkningens formål

Betænkningen tjener det formål at sikre forordningens korrekte gennemførelse i dansk ret, herunder at analysere rammerne for både *indførelse* og *opretholdelse* af nationale særregler, når forordningen anvendes den 25. maj 2018.

Betænkningens analyser vil endvidere danne grundlag for udarbejdelsen af en ny version af persondataloven og følgelove med konsekvensrettelser.

Betænkningen skal således tjene som et centralt fortolkningsbidrag til det videre arbejde med forslagene.

Betænkningen er endelig tiltænkt at være det retlige grundlag for udarbejdelse af praktisk anvendelige vejledninger, som man eksempelvis kender fra den eksisterende vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsvejledningen).

1.5. Betænkningens opbygning

Betænkningens *første del* indeholder en nærmere analyse af den gældende retstilstand og forordningens bestemmelser, herunder forordningens rammer for nationale særregler. Første del af betænkningen er opdelt i kapitler, som svarer til kapitlerne i databeskyttelsesforordningen.

Kapitlerne er endvidere opdelt i afsnit, der hovedsageligt er opdelt efter artiklerne i forordningen.

Hvert afsnit indeholder – efter en indledning – en redegørelse for gældende ret i databeskyttelsesdirektivet og persondataloven med inddragelse af relevante kilder såsom praksis fra EU-Domstolen og Datatilsynet, diverse udtalelser fra Artikel 29-gruppen[2] samt Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger.

Herefter er der i hvert afsnit oftest under overskriften "databeskyttelsesforordningen" en nærmere analyse af de pågældende bestemmelser i forordningen.

Endvidere indeholder hvert afsnit et overvejelsesafsnit. Disse afsnit indeholder oftest en summarisk konklusion på, om bestemmelserne i forordningen svarer til, hvad der følger af gældende ret, eller om der er tale om en nyskabelse. Eksempelvis redegøres der i afsnittene vedrørende den registreredes rettigheder for, hvornår den registreredes rettigheder adskiller sig fra den gældende retstilstand efter persondataloven og databeskyttelsesdirektivet, samt hvornår der er tale om "nye" rettigheder. I overvejelsesafsnittene overvejes det også summarisk om en eventuel særlig dansk retstilstand vil kunne opretholdes.

At betænkningen indeholder en udførlig analyse af gældende ret i forhold til bestemmelserne i forordningen tjener hovedsageligt to formål. For det første tjener analysen som et bidrag til fortolkningen af forordningen, herunder særligt med en afklaring af, hvor forord-

[2] I medfør af databeskyttelsesdirektivet er der nedsat en "gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger" – den såkaldte "Artikel 29-gruppe". Artikel 29-gruppen er rådgivende og uafhængig og består af en repræsentant for den eller de tilsynsmyndigheder, som hver medlemsstat har udpeget, og af en repræsentant for den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne, samt af en repræsentant for Kommissionen. Artikel 29-gruppen har vedtaget en række henstillinger, udtalelser og notater, som bl.a. vedrører spørgsmålet om overførsel af personoplysninger fra EU-landene til andre lande.

ningen svarer til gældende ret, og hvor der er tale om en nyskabelse. For det andet udgør beskrivelsen af gældende ret et (nødvendigt) grundlag for overvejelser om, i hvilket omfang der er behov for at tilpasse danske regler til forordningen, herunder hvad det nationale råderum for at fastsætte national særlovgivning er.

Betænkningens *anden del* indeholder en analyse af konsekvenserne for gældende dansk særlovgivning i forhold til forordningen inden for samtlige ministeriers område. Anden del af betænkningen indeholder en samlet overordnet vurdering af gældende ret på de enkelte ministeriers ressortområde i forhold til forordningen, inklusiv et bilag med angivelse af de relevante love om behandling af personoplysninger og deres ophæng i databeskyttelsesforordningen.

De enkelte ministerier har således gennemgået lovgivningen på ministeriets ressortområde med henblik på at identificere bestemmelser, der regulerer behandling af personoplysninger eller i øvrigt har relation til forhold, som databeskyttelsesforordningen regulerer, herunder f.eks. den registreredes rettigheder. Ministerierne har i samarbejde med Justitsministeriet i den forbindelse vurderet, om de pågældende bestemmelser kan opretholdes, når databeskyttelsesforordningen anvendes fra den 25. maj 2018.

Ministerierne har i samarbejde med Justitsministeriet vurderet, at de fleste af de identificerede bestemmelser om behandling af personoplysninger mv. kan opretholdes, når databeskyttelsesforordningen finder anvendelse.

I bilagene til kapitlerne fra de enkelte ministerier er oplistet de hovedlove på ministeriets område, hvor ministerierne har identificeret bestemmelser, som regulerer behandling af personoplysninger i selve loven. Ved de enkelte love er kort anført, hvilke typer af behandlinger loven regulerer, samt hvilke bestemmelser i databeskyttelsesforordningen, der vurderes at hjemle behandlingerne fra den 25. maj 2018. Af bilagene fremgår kun det enkelte ministeriums love. Ministerierne har dog også foretaget en gennemgang af, om bekendtgørelser kan opretholdes, når forordningen finder anvendelse.

1.6. Betænkningens konklusioner

Analysearbejdet har vist, at forordningen i vidt omfang svarer til den gældende retstilstand efter persondataloven og databeskyttelsesdirektivet med tilhørende praksis fra bl.a. EU-Domstolen og Datatilsynet. Bl.a. svarer forordningens centrale bestemmelser om anvendelsesområde, definitioner, principper for behandling af personoplysninger, behandlingsregler, de registreredes rettigheder og behandlingssikkerhed i stort omfang til gældende ret efter persondataloven og databeskyttelsesdirektivet.

Derudover indeholder forordningen bestemmelser, som er en nyskabelse i forhold til den gældende retstilstand. Dette er eksempelvis bestemmelserne om databeskyttelsesrådgivere, konsekvensanalyse og fortegnelser over behandlingsaktiviteter samt en udtrykkelig bestemmelse om "data protection by design".

På den baggrund vil der for myndigheder og private organisationer, der i forvejen lever op til persondataloven, ikke med forordningen være tale om omfattende ændringer.

Der vil sikkert være offentlige myndigheder og private organisationer mv., som ikke på nuværende tidspunkt opfylder alle krav i persondataloven og derfor ikke er "compliant" med gældende ret. For disse offentlige myndigheder og private er det oplagt, at der med databeskyttelsesforordningen er skabt "awareness" eller "bevidsthed" omkring betydningen af beskyttelse af personoplysninger. Dette er nok en konsekvens af, at EU-lovgiver nu har vedtaget en generel forordning om databeskyttelse, som bl.a. indeholder mulighed for at pålægge større bøder for overtrædelse af forordningens bestemmelser.[3]

1.7. Betænkningens retlige status

Betænkningens analyser er baseret på eksisterende retskilder. Betænkningen vil således ikke stå alene som fortolkningsbidrag *fremover*.

Hvor retstilstanden ikke kan anses for entydig, indeholder betænkningen i vidt omfang forslag til *mulige løsninger*.

Det må forventes, at fortolkningen af forordningen på flere punkter i de kommende år vil blive udviklet gennem praksis fra bl.a. det med forordningen nyoprettede Europæiske Databeskyttelsesråd, EU-Domstolen, de danske domstole og Datatilsynet.

Den nuværende retstilstand er f.eks. baseret på meget få domme, og det må forventes, at der fremover vil komme flere domme fra bl.a. EU-Domstolen.

I det omfang, der kommer bindende afgørelser fra EU-Domstolen, nationale domstole, Databeskyttelsesrådet og den uafhængige tilsynsmyndighed mv., skal betænkningens analyser naturligvis læses i lyset af den nye praksis.

[3] Se i den forbindelse tilsvarende overvejelser hos professor Peter Blume i Den nye persondataret, Persondataforordningen, Jurist- og Økonomforbundets Forlag, 2016, s. 195 (herefter "Peter Blume, Den nye persondataret (2016)") og i Juristen, 2016, nr. 4, s. 169-176 (særligt s. 175).

1.8. Nærmere om forordningens gennemførelse i dansk ret

Ifølge artikel 288 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF) er der forskel på, om et område harmoniseres ved et direktiv eller en forordning.

Det følger af artikel 288, 3. pkt., i TEUF, at et direktiv med hensyn til det tilsigtede mål er bindende for enhver medlemsstat, som det rettes til, men overlader det til de nationale myndigheder at bestemme form og midler for gennemførelsen.

Det indebærer bl.a., at et direktiv, som indeholder rettigheder og pligter for borgerne og virksomhederne, skal gennemføres enten ved lov eller ved en bekendtgørelse med hjemmel i lov.[4]

Til forskel fra et direktiv er en forordning ifølge TEUF artikel 288, 1. og 2. pkt., almengyldig, og er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

En forordning virker således som en lov i medlemsstaterne, og den gælder i den form, som den er vedtaget, og den må som udgangspunkt ikke gennemføres i national ret. Medlemsstaterne kan således ikke udstede bindende fortolkningsregler, selv om forordningen måtte give anledning til tvivl.[5] Medlemsstaterne vil imidlertid kunne udstede vejledninger, der efter deres karakter ikke er bindende, jf. f.eks. vejledning nr. 145 af 21. december 2006 om dyretransportforordningen (forordning nr. 1/2005).

Ud over, at en forordning som udgangspunkt ikke må gennemføres i medlemsstaterne, vil medlemsstaternes modstridende lovgivning blive fortrængt af en forordning, hvorfor det vil være nødvendigt at ophæve denne lovgivning således, at der ikke opstår nogen usikkerhed om retstilstanden. Ophævelsen skal ske enten ved lov eller ved bekendtgørelse med hjemmel i lov. Forordningen vil således ikke i sig selv være en tilstrækkelig hjemmel til at ophæve lovgivning.[6]

Ofte skal der dog, som det er tilfældet med databeskyttelsesforordningen, udfærdiges supplerende nationale bestemmelser, f.eks. om hvilken myndighed der skal administrere forordningen, sanktioner og kontrol. Som det endvidere er tilfældet med databeskyttelsesforordningen, hænder det også, at en forordning efter sit indhold forudsætter, at medlemsstaterne skal fastsætte nærmere regler, der gennemfører forordningens mere overordnede regulering. På dette punkt vil forordningen herved svare til et direktiv.

[4] Nina Holst-Christensen, Skriftlig jura – Den juridiske fremstilling, EU-Lovteknik, 2013, s. 470 f.
[5] Nina Holst-Christensen, Skriftlig jura – Den juridiske fremstilling, EU-Lovteknik, 2013, s. 487 f. og Jens Hartig Danielsen m.fl., EU-retten, 6. udgave, 2014, s. 96.
[6] Nina Holst-Christensen, Skriftlig jura – Den juridiske fremstilling, EU-Lovteknik, 2013, s. 489.

Der kan i forbindelse med udarbejdelse af den supplerende danske lovgivning opstå behov for at gengive dele af eller hele forordningen i en lov eller bekendtgørelse. EU-Domstolen anerkender, at en sådan gengivelse kan finde sted, blot det udtrykkeligt anføres i loven eller bekendtgørelsen, at der er tale om en gengivelse af en forordning.[7] I databeskyttelsesforordningens præambelbetragtning nr. 8 er det præciseret, at forordningens bestemmelser kan gengives i nationale regler, i det omfang det er nødvendigt af hensyn til sammenhængen og for at gøre de nationale bestemmelser forståelige for de personer, som de finder anvendelse på.

Som følge af databeskyttelsesforordningens almengyldighed vil forordningen som udgangspunkt fortrænge danske regler, der regulerer de samme forhold som forordningen.

Danmark er dermed forpligtet til at indrette dansk lovgivning i overensstemmelse med forordningens bestemmelser med virkning fra den 25. maj 2018.

Som det ses på baggrund af gennemgangen af forordningens bestemmelser i denne betænkning, er der imidlertid en række undtagelser i databeskyttelsesforordningen til dette udgangspunkt, idet visse regler i forordningen bestemmer, at medlemsstaterne inden for nærmere bestemte områder enten skal eller kan fastsætte nationale regler.

Bestemmelserne i forordningen, hvorefter medlemsstaterne kan eller skal fastsætte nationale regler, kan opdeles i fire forskellige kategorier.

I den *ene* kategori er der en række bestemmelser i forordningens artikel 6, stk. 2 og 3, artikel 9, stk. 2-4, artikel 87, 88 og 90, der bemyndiger medlemsstaterne til at fastsætte mere specifikke bestemmelser inden for rammerne af forordningens harmonisering. Medlemsstaterne har mulighed for at udnytte dette nationale råderum, men de er ikke forpligtede hertil.

En *anden* kategori er bestemmelserne i forordningens artikel 8, stk. 1, artikel 36, stk. 5, artikel 37, stk. 4, artikel 49, stk. 5, artikel 80, stk. 2, og artikel 83, stk. 7 og 9, der giver medlemsstaterne eksplicitte muligheder for at foretage nogle valg ved lov eller regler fastsat med hjemmel i lov. F.eks. kan medlemsstaterne efter artikel 8, stk. 1, vælge en lavere aldersgrænse end 16 år for, hvornår et barn kan give samtykke til behandling af personoplysninger i forbindelse med udbud af informationssamfundstjenester direkte til børn. Endvidere kan medlemsstaterne eksempelvis efter artikel 49, stk. 5, under visse betingelser

[7] Nina Holst-Christensen, Skriftlig jura – Den juridiske fremstilling, EU-Lovteknik, 2013, s. 487 f. I det tilfælde, hvor forordningen gengives, skal det fremgå af en note, at bestemmelserne stammer fra en forordning, og at gengivelsen er begrundet i praktiske hensyn.

udtrykkeligt fastsætte grænser for overførsel af særlige kategorier af oplysninger til et tredjeland eller en international organisation.

En *tredje* kategori er bestemmelserne i forordningens artikel 23 og artikel 89, stk. 2 og 3, hvorefter medlemsstaterne *kan* fastsætte regler om begrænsninger og undtagelser til en række forpligtelser og rettigheder, f.eks. undtagelser til eller begrænsninger i forpligtelsen til at give den registrerede oplysninger i forbindelse med indsamling af personoplysninger eller begrænsninger i retten for den registrerede til indsigt i oplysninger om sig selv.

Den sidste, *fjerde* kategori er bestemmelserne i forordningens artikel 43, stk. 1, artikel 51, stk. 1 og 3, artikel 52, stk. 2-4, artikel 53, stk. 1, artikel 54, stk. 1, artikel 84 og artikel 85, stk. 1 og 2, som *skal* gennemføres ved lov af medlemsstaterne. Efter artikel 51, stk. 1 og 3, skal medlemsstaterne eksempelvis fastsætte bestemmelser om udpegning eller oprettelse af en eller flere uafhængige tilsynsmyndigheder.

Forpligtelserne og mulighederne i forordningen for medlemsstaterne til at fastsætte nationale regler modsvares i et vist omfang af forpligtelser for medlemsstaterne i forordningens artikel 49, stk. 5, artikel 51, stk. 4, artikel 83, stk. 9, artikel 84, artikel 85, stk. 1 og 2, artikel 88, stk. 3, og artikel 90, stk. 2, til at give Kommissionen meddelelse om de regler, de fastsætter (notifikationsforpligtelser). Medlemsstaterne skal således f.eks., hvis de benytter muligheden i artikel 49, stk. 5, for udtrykkeligt at fastsætte grænser for overførsel af særlige kategorier af oplysninger til et tredjeland mv., efter samme bestemmelse give Kommissionen meddelelse herom, ligesom medlemsstaterne efter artikel 51, stk. 4, senest den 25. maj 2018 skal give Kommissionen meddelelse om de bestemmelser, de vedtager på baggrund af forpligtelsen hertil i artikel 51, stk. 1 og 3.

Udgangspunktet for persondataloven er, at de regler, der gælder inden for lovens almindelige anvendelsesområde efter lovens § 1, stk. 1, som svarer til forordningens anvendelsesområde, skal ophæves.

Det betyder som udgangspunkt, at regler i den gældende persondatalov ikke kan bestå efter den 25. maj 2018, hvorfra forordningen skal anvendes.

Dog er der som anført bestemmelser i forordningen, som skal gennemføres i dansk ret, og bestemmelser, som giver mulighed for at fastsætte særlige danske regler af mere generel og tværgående karakter. Nogle af sådanne danske regler fastsættes mest hensigtsmæssigt i en generel lov såsom en ændret eller ny lov om behandling af personoplysninger, f.eks. regler om oprettelse af en uafhængig dansk tilsynsmyndighed. Det er som nævnt i databeskyttelsesforordningens præambelbetragtning nr. 8 præciseret, at forordningens bestemmelser kan

gengives i nationale regler, i det omfang det er nødvendigt af hensyn til sammenhængen og for at gøre de nationale bestemmelser forståelige for de personer, som de finder anvendelse på.

Der vil på den baggrund fortsat være behov for en generel lov om behandling af personoplysninger, hvori sådanne bestemmelser af mere generel, tværgående karakter fastsættes. Herudover kan der – hvis der er et politisk ønske herom – være behov at videreføre regler i persondataloven, der i medfør af lovens § 1 gælder på områder, som falder uden for forordningens anvendelsesområde, og dermed ikke skal ophæves eller ændres som følge af forordningen.

2. Forordningens kapitel I: Generelle bestemmelser

2.1. Anvendelsesområde, artikel 2 og 3

2.1.1. Præsentation

Persondatalovens materielle anvendelsesområde følger af lovens § 1. I lovens § 2 følger en række undtagelser til anvendelsesområdet. Derudover følger persondatalovens territoriale anvendelsesområde af lovens § 4.

Da persondataloven gennemfører databeskyttelsesdirektivet, er anvendelsesområdet særligt fastsat under hensyn til direktivets anvendelsesområde. Dog gælder persondataloven i videre omfang end forudsat efter direktivet.

Databeskyttelsesforordningens anvendelsesområde, som følger af forordningens artikel 2 om det materielle anvendelsesområde og artikel 3 om det territoriale anvendelsesområde, svarer i vidt omfang til direktivets anvendelsesområde.

2.1.2. Gældende ret

2.1.2.1. Materielt anvendelsesområde – databeskyttelsesdirektivet

Databeskyttelsesdirektivets bestemmelser anvendes ifølge direktivets artikel 3, stk. 1, på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb, samt på ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Definitionen af begreberne personoplysning, behandling og register følger af direktivets artikel 2, litra a- litra c.

Af direktivets artikel 3, stk. 2, følger en række undtagelser i forhold til de behandlinger af personoplysninger, der er omfattet af stk. 1.

2.1.2.2. Aktiviteter, der ikke er omfattet af fællesskabsretten

Ifølge artikel 3, stk. 2, 1. pind, gælder direktivet ikke for behandling af personoplysninger, som iværksættes med henblik på udøvelse af aktiviteter, der ikke er omfattet af fællesskabsretten, som *f.eks.* de aktiviteter, der er fastsat i (dagældende) afsnit V og VI i traktaten om Den Europæiske Union, og under ingen omstændigheder for behandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed (herunder statens økonomiske interes-

ser, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område.[8]

I sag C-101/01, Lindqvist, dom af 6. november 2003, undersøgte EU-Domstolen, om behandling af personoplysninger som led i frivillige og religiøse aktiviteter kunne anses for at være aktiviteter, der ikke var omfattet af fællesskabsretten i den forstand, hvori udtrykket er anvendt i direktivets artikel 3, stk. 2, 1. pind.[9]

I sagen havde en person oprettet hjemmesider på internettet for at gøre det let for menighedsmedlemmer at forberede konfirmation. Hjemmesiderne indeholdt oplysninger om bl.a. 18 kolleger, herunder med navn og oplysning om kollegernes arbejdsopgaver og fritidsvaner. I flere tilfælde var også deres telefonnummer og familieforhold anført. Endelig var der om en af kollegerne oplyst, at hun havde beskadiget foden og var delvist sygemeldt.

I sagen henviste EU-Domstolen bl.a. til, at de aktiviteter, der er nævnt som eksempler i denne bestemmelse, dvs. aktiviteter vedrørende den offentlige sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område, under alle omstændigheder er statens eller statslige myndigheders aktiviteter og ikke har noget at gøre med området for den enkelte borgers aktiviteter.[10]

EU-Domstolen fastslog, at de aktiviteter, der er nævnt som eksempler i direktivets artikel 3, stk. 2, 1. pind, skal fastlægge rækkevidden af de undtagelser, der er fastsat heri, således at denne undtagelse kun finder anvendelse på aktiviteter, der udtrykkeligt er nævnt i bestemmelsen, eller som kan henføres til samme kategori.[11]

Om baggrunden for domstolens konklusion fremgår det, at det retsgrundlag i traktaten, som databeskyttelsesdirektivet er udstedt med hjemmel i (dagældende artikel 100 A i EF-traktaten), ikke forudsætter, at der altid skal foreligge en tilknytning til den frie bevægelighed mellem medlemsstater.

I præmisserne om baggrunden for EU-Domstolens konklusion henvises bl.a. til de forenede sager C-465/00, C-138/01 og C-139/01, Österreichischer Rundfunk m.fl., dom af 20. maj 2003.[12]

[8] Herved også databeskyttelsesdirektivets præambelbetragtning nr. 12 og 13.
[9] Sag C-101/01, Lindqvist-sagen, præmis 39.
[10] Sag C-101/01, Lindqvist-sagen, præmis 43.
[11] Sag C-101/01, Lindqvist-sagen, præmis 44.
[12] Sag C-101/01, Lindqvist-sagen, præmis 40-41.

Denne sag vedrørte en pligt i østrigsk ret, som offentlige institutioner, der er undergivet Rechnungshofs (den østrigske rigsrevision) revision, havde til at give meddelelse om de indkomster og pensioner over en bestemt størrelse, som de udbetalte til deres ansatte og tidligere ansatte, samt om modtagernes navne med henblik på udarbejdelse af en årsberetning, der skulle forelægges for Nationalrat (Nationalrådet), Bundesrat (Forbundsrådet) og for Landtagen (delstatsparlamenterne) og stilles til rådighed for offentligheden.

EU-Domstolen fastslog, at det, der er afgørende for, om det er berettiget at anvende det pågældende retsgrundlag i traktaten til at udstede direktivet, er, at retsakten har til formål at skabe bedre vilkår for det indre markeds oprettelse og funktion. Endvidere fremgår det, at anvendelsen af databeskyttelsesdirektivet således ikke afhænger af, om der konkret er en tilstrækkelig tilknytning til udøvelsen af de grundlæggende rettigheder i traktaten, navnlig arbejdskraftens frie bevægelighed. Risikoen ved en modsat fortolkning ville ifølge domstolen være, at grænserne for anvendelsesområdet ville blive særdeles usikre og uberegnelige, hvilket ville være uforeneligt med direktivets grundlæggende formål, der er at foretage en indbyrdes tilnærmelse af medlemsstaternes nationale love og administrative bestemmelser for at fjerne de hindringer for det indre markeds funktion, der netop hidrører fra forskellene i de nationale lovgivninger.

Desuden fremgår det, at domstolens forståelse af direktivets artikel 3, stk. 1, bl.a. bekræftes af bestemmelsens ordlyd, som indeholder en meget bred definition af direktivets anvendelsesområde, idet den ikke gør anvendelsen af beskyttelsesreglerne betinget af, at behandlingen faktisk har tilknytning til den frie bevægelighed mellem medlemsstaterne. Desuden bekræftes forståelsen ifølge domstolen af direktivets artikel 8, stk. 2, som omhandler behandlingen af særlige kategorier af oplysninger, og navnlig undtagelserne i stk. 2, litra d, som vedrører behandling, der foretages af en stiftelse, en forening eller andet almennyttigt organ, hvis sigte er af politisk, filosofisk, religiøs eller faglig art. Domstolen henviser yderligere til de formål, der kommer til udtryk i direktivets artikel 7, litra a og e, og i artikel 13, litra e og f.[13]

I Lindqvist-sagen fastslog Domstolen bl.a. på baggrund af dommen i sagerne Österreichischer Rundfunk m.fl., at udtrykket, "aktiviteter, der ikke er omfattet af fællesskabsretten", ikke skal fortolkes således, at det i hvert enkelt tilfælde skal efterprøves, om den pågældende specifikke aktivitet direkte påvirker den frie bevægelighed mellem medlemsstaterne.[14] Det fremgår således tydeligt, at det bl.a. ikke er afgørende for direktivets anvendelse, om der er en grænseoverskridende aktivitet.

[13] De forenede sager C-465/00, C-138/01 og C-139/01, Österreichischer Rundfunk m.fl., præmis 41-46.
[14] Sag C-101/01, Lindqvist-sagen, præmis 42.

2.1.2.3. Aktiviteter af rent privat karakter

Databeskyttelsesdirektivet gælder ifølge direktivets artikel 3, stk. 2, 2. pind, ikke for behandling af personoplysninger, som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter. I direktivets præambelbetragtning nr. 12 er det anført, at dette f.eks. er korrespondance og føring af adressefortegnelser.

For nærmere om denne undtagelse henvises til afsnit 2.2. om rent privat karakter.

2.1.2.4. Territorialt anvendelsesområde

I databeskyttelsesdirektivets artikel 4 er der regler om direktivets territoriale anvendelsesområde.

Ifølge direktivets artikel 4, stk. 1, litra a, anvender medlemsstaterne de nationale bestemmelser, som de vedtager til gennemførelse af direktivet, på behandling af personoplysninger, der foretages som led i en virksomheds eller et organs aktiviteter inden for den medlemsstats område, hvor den dataansvarlige er *etableret*. For en dataansvarlig, som er etableret på flere medlemsstaters område, følger det endvidere af bestemmelsen, at denne skal træffe de nødvendige foranstaltninger til at sikre, at hver af disse virksomheder eller organer opfylder kravene i den gældende nationale lovgivning.

Definitionen af en dataansvarlig følger af direktivets artikel 2, litra d.

I direktivets præambelbetragtning nr. 19 er det nærmere angivet, at der ved etablering på en medlemsstats område forstås faktisk udøvelse af aktiviteter gennem en mere permanent struktur. Endvidere er det heri angivet, at den pågældende strukturs retlige form, hvad enten det blot er en filial eller et datterselskab med status som juridisk person, ikke har afgørende betydning i denne forbindelse. Det er tillige anført, at en dataansvarlig, som er etableret på flere medlemsstaters område, især i form af datterselskaber, navnlig for at undgå omgåelse, skal sikre sig, at hver enkelt struktur opfylder kravene i den gældende nationale lovgivning.

I sag C-131/12, Google Spain, dom af 13. maj 2014, har EU-Domstolen fastslået, at der ikke skal meget til, før der er tale om behandling af personoplysninger, der foretages *som led i en virksomheds aktiviteter*, når en dataansvarlig i et tredjeland etablerer en filial eller et datterselskab i en medlemsstat, når aktiviteterne hos henholdsvis den dataansvarlige og henholdsvis filialen eller databehandleren er uløseligt forbundne.[15] I sagen fandt EU-Domstolen bl.a., at databeskyttelsesdirektivets artikel 4, stk. 1, litra a, skal fortolkes såle-

[15] Sag C-131/12, Google Spain, præmis 50-60.

des, at en behandling af personoplysninger foretages som led i aktiviteter, der inden for en medlemsstats område udføres af en dataansvarligs virksomhed eller organ som omhandlet i bestemmelsen, når en søgemaskineudbyder etablerer en filial eller et datterselskab i en medlemsstat, der skal sørge for reklame og salg af reklameplads i søgemaskinen, og hvis aktivitet er rettet mod indbyggerne i denne medlemsstat.[16]

I sag C-230/14, Weltimmo, dom af 1. oktober 2015, har EU-Domstolen udtalt, at der med henblik på at fastslå, om en dataansvarlig er *etableret* i en medlemsstat, bør foretages en vurdering af, i hvor høj grad strukturen er permanent, og i hvilken grad der faktisk udøves aktiviteter i denne anden medlemsstat, idet der i den forbindelse skal tages hensyn til den specifikke karakter af de pågældende økonomiske aktiviteter og de pågældende tjenesteydelser, hvilket navnlig gør sig gældende for virksomheder, der udelukkende udbyder tjenesteydelser på nettet.[17] Endvidere må det ifølge domstolen i den henseende bl.a. – i lyset af det formål, der forfølges med databeskyttelsesdirektivet, om at sikre en effektiv og fuldstændig beskyttelse af retten til privatlivets fred og undgå omgåelse – antages, at tilstedeværelsen af en enkelt repræsentant under visse omstændigheder kan være tilstrækkeligt til at udgøre en permanent struktur, såfremt denne repræsentant optræder med en tilstrækkelig grad af stabilitet og under tilstedeværelse af de midler, der er nødvendige for at kunne levere de pågældende konkrete tjenesteydelser i den pågældende medlemsstat.[18] Desuden må det ifølge domstolen med henblik på at realisere det nævnte formål antages, at begrebet 'etablering', som omhandlet i databeskyttelsesdirektivet, omfatter enhver, selv minimal, reel og faktisk aktivitet, der udøves via en permanent struktur.[19]

Endvidere fremgår det af EU-Domstolens dom i sag C-191/15, Amazon, dom af 28. juli 2016, at selv om det ikke er udelukket, at en virksomhed i et tredjeland, der hverken har et datterselskab eller en filial i en medlemsstat, kan anses for etableret i Unionen, er den blotte omstændighed, at der er adgang til den pågældende virksomheds hjemmeside fra denne medlemsstat, ikke tilstrækkeligt for at anse virksomheden for omfattet af direktivets artikel 4, stk. 1, litra a.[20]

Mens databeskyttelsesdirektivets artikel 4, stk. 1, litra a, vedrører dataansvarlige *etableret inden for EU*, omhandler artikel 4, stk. 1, litra b og c, dataansvarlige *etableret i et tredjeland*.

[16] Sag C-131/12, Google Spain, præmis 60.
[17] Sag C-230/14, Weltimmo, præmis 29.
[18] Sag C-230/14, Weltimmo, præmis 30.
[19] Sag C-230/14, Weltimmo, præmis 31.
[20] Sag C-191/15, Amazon, præmis 76.

Ifølge artikel 4, stk. 1, litra b, anvender medlemsstaterne de nationale bestemmelser, som de vedtager til gennemførelse af direktivet, på behandling af personoplysninger, der foretages af en dataansvarlig, der ikke er etableret på den pågældende medlemsstats område, men på et sted, hvor dens nationale lovgivning gælder i henhold til folkeretten.

Endvidere anvender medlemsstaterne ifølge artikel 4, stk. 1, litra c, de nationale bestemmelser, som de vedtager til gennemførelse af direktivet, på behandling af personoplysninger, der foretages af en dataansvarlig, der ikke er etableret på Fællesskabets område, og som med henblik på behandling af personoplysninger anvender midler, det være sig elektroniske eller ikke-elektroniske, som befinder sig på den pågældende medlemsstats område, medmindre disse midler kun benyttes med henblik på forsendelse gennem Det Europæiske Fællesskabs område. I sådanne tilfælde skal den dataansvarlige ifølge direktivets artikel 4, stk. 2, udpege en repræsentant, der er etableret på den pågældende medlemsstats område, uden at dette i øvrigt berører eventuelle retslige skridt mod den dataansvarlige selv.

2.1.2.5. Direktivet i forhold til Færøerne og Grønland

I Registerudvalgets betænkning nr. 1345 adresseres det særlige spørgsmål om databeskyttelsesdirektivet i forhold til Færøerne og Grønland. Af betænkningen fremgår det, at det under hensyn til Grønlands og Færøernes særlige retsstilling i relation til Det Europæiske Fællesskab, jf. artikel 136 a og 227 i traktaten om Det Europæiske Fællesskab, må Færøerne og Grønland efter Registerudvalgets opfattelse antages at skulle anses for tredjelande i direktivets forstand.[21] I den forbindelse kan det bemærkes, at Færøerne efterfølgende i henhold til databeskyttelsesdirektivets artikel 25, stk. 6, er godkendt af Kommissionen som et tredjeland med et tilstrækkeligt beskyttelsesniveau.

2.1.2.6. Materielt anvendelsesområde – persondataloven

I persondatalovens kapitel 1 fastlægges lovens materielle anvendelsesområde. Lovens territoriale anvendelsesområde følger af lovens kapitel 3.

Ifølge persondatalovens § 1, stk. 1, gælder loven for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register. Det fremgår af bemærkningerne til persondataloven, at bestemmelsen fastlægger lovens almindelige anvendelsesområde under hensyn til anvendelsesområdet i databeskyttelsesdirektivets artikel 3.[22]

[21] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 224.
[22] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 1, stk. 1.

Begreberne 'personoplysninger', 'behandling' og 'register' er nærmere defineret i persondatalovens § 3, nr. 1-3.

Herudover gælder reglerne i persondataloven også på en række områder, jf. lovens § 1, stk. 2-5 og 8, som ikke er forudsat efter direktivet. Ifølge persondatalovens § 1, stk. 2, gælder loven – dog ikke lovens kapitel 8 og 9 – for anden ikke-elektronisk systematisk behandling, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden. Endvidere gælder persondatalovens § 5, stk. 1-3, §§ 6-8, § 10, § 11, stk. 1, § 38 og § 40 ifølge lovens § 1, stk. 3, for manuel videregivelse af personoplysninger til en anden forvaltningsmyndighed.

Persondataloven gælder også i et vist omfang for oplysninger om virksomheder mv. Ifølge lovens § 1, stk. 4, gælder loven for behandling af oplysninger om virksomheder mv., jf. § 1, stk. 1 og 2, som foretages for kreditoplysnings- og advarselsbureauer. Det fremgår af bemærkningerne til persondataloven, at det med henvisningen i § 1, stk. 4, til stk. 1 og 2, præciseres, at udvidelsen af lovens område til også at angå behandling af oplysninger om juridiske personer kun gælder for så vidt angår de behandlingsformer, som i øvrigt er omfattet af loven.[23] Justitsministeren kan i medfør af persondatalovens § 1, stk. 6, uden for de i stk. 4 nævnte tilfælde bestemme, at lovens regler helt eller delvis skal finde anvendelse på behandling af oplysninger om virksomheder mv., som udføres for private.

Persondataloven gælder tillige ifølge lovens § 1, stk. 5, for offentlige myndigheders videregivelse til kreditoplysningsbureauer af oplysninger om virksomheder mv. angående gæld til det offentlige, hvis oplysningerne behandles helt eller delvis elektronisk eller er eller vil blive indeholdt i et register, jf. henvisningen til stk. 1 i bestemmelsen. Vedkommende minister kan i medfør af persondatalovens § 1, stk. 7, uden for de i stk. 5 nævnte tilfælde bestemme, at lovens regler helt eller delvis skal finde anvendelse på behandling af oplysninger om virksomheder mv., som udføres for den offentlige forvaltning.

Endelig gælder persondataloven ifølge lovens § 1, stk. 8, for enhver form for behandling af personoplysninger i forbindelse med tv-overvågning. Det følger af bemærkningerne til persondataloven, at bestemmelsen er indsat med henblik på, at lovens område skal omfatte behandling af personoplysninger i forbindelse med offentlige myndigheders tv-

[23] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 1, stk. 3.

overvågning med analogt udstyr og tv-overvågning med analogt udstyr, der foretages for private, hvor oplysningerne ikke behandles systematisk.[24]

2.1.2.7. Undtagelser fra det materielle anvendelsesområde
Persondatalovens § 2 indeholder regler om undtagelser fra persondatalovens materielle anvendelsesområde.

Ifølge lovens § 2, stk. 1, går regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, forud for reglerne i persondataloven. Det indebærer bl.a., at sundhedspersoners videregivelse af fortrolige oplysninger afgøres efter sundhedsloven, at reglerne om tavshedspligt i den finansielle lovgivning går forud for persondataloven, samt at spørgsmål om videregivelse af oplysninger i ansøgningssager i den offentlige sektor reguleres af forvaltningslovens § 29.

Bestemmelsen indebærer, at persondataloven finder anvendelse, hvis regler om behandling af personoplysninger i anden lovgivning giver den registrerede en dårligere retsstilling. Det fremgår imidlertid af bemærkningerne til persondataloven, at dette ikke gælder, hvis den dårligere retsstilling har været tilsigtet og i øvrigt ikke strider mod databeskyttelsesdirektivet.[25]

Endvidere følger det af persondatalovens § 2, stk. 2, at loven ikke finder anvendelse, hvis det vil være i strid med informations- og ytringsfriheden, jf. Den Europæiske Menneskerettighedskonventions artikel 10. Herom fremgår det af bemærkningerne til persondataloven, at bestemmelsen er indsat for at fjerne enhver tvivl om, at der ikke med persondataloven gennemføres en regulering, der indebærer begrænsninger i den informations- og ytringsfrihed, som følger af den nævnte bestemmelse i Den Europæiske Menneskerettighedskonvention.[26]

Af persondatalovens § 2, stk. 3, følger det, at loven ikke gælder for behandlinger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter. Bestemmelsen svarer til undtagelsen fra anvendelsesområdet i databeskyttelsesdirektivet, jf. direktivets artikel 3, stk. 2, 2. pind.

---

[24] Lovforslag nr. L 162 af 28. februar 2007, FT 2006/07, om ændring af lov om forbud mod tv-overvågning m.v. og lov om behandling af personoplysninger (Udvidelse af adgangen til tv-overvågning og styrkelse af retsbeskyttelsen ved behandling af personoplysninger i forbindelse med tv-overvågning), de specielle bemærkninger til § 2, nr. 1.
[25] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 2, stk. 1.
[26] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 2, stk. 2.

Persondataloven finder ifølge lovens § 2, stk. 4, desuden ikke anvendelse på behandling af oplysninger, der foretages for Folketinget og institutioner med tilknytning dertil.

Derudover er der i persondatalovens § 2, stk. 5-9, en række undtagelser vedrørende medier-nes behandling af oplysninger. Det fremgår af bemærkningerne til persondataloven, at disse undtagelser er fastsat inden for rammerne af direktivet, herunder direktivets artikel 9.[27]

Efter stk. 5 finder loven ikke anvendelse for behandlinger, der er omfattet af lov om massemediers informationsdatabaser. Persondataloven finder efter stk. 6 og 7 heller ikke anvendelse på de informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte periodiske skrifter eller lyd- og billedprogrammer, der er omfattet af medieansvarslovens § 1, nr. 1 eller 2, eller hvori der udelukkende er indlagt allerede offentliggjorte tekster, billeder og lydprogrammer, der omfattes af medieansvarslovens § 1, nr. 3. Undtagelserne i stk. 7 og 8 gælder kun, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen. Endvidere finder loven efter stk. 8-9 ikke anvendelse på manuelle arkiver over udklip fra offentliggjorte, trykte artikler, som udelukkende behandles i journalistisk øjemed, og for behandling af oplysninger, som i øvrigt udelukkende finder sted i journalistisk øjemed eller udelukkende sker med henblik på kunstnerisk eller litterær virksomhed. Bestemmelserne i persondatalovens §§ 41, 42 og 69 gælder dog uanset undtagelserne i § 2, stk. 5-9.

Endelig gælder persondataloven ifølge lovens § 2, stk. 10, ikke for behandlinger, der udføres for politiets og forsvarets efterretningstjenester. Bestemmelsen har sin baggrund i databeskyttelsesdirektivets artikel 3, stk. 2, 1. pind.

2.1.2.8. Territorialt anvendelsesområde

I overensstemmelse med databeskyttelsesdirektivets artikel 4 følger det af persondatalovens § 4, stk. 1, at loven geografisk gælder for behandling af oplysninger, som udføres for en dataansvarlig, der er etableret i Danmark, hvis aktiviteterne finder sted inden for Det Europæiske Fællesskabs område.

Bestemmelsen omfatter kun dataansvarlige etableret på dansk område. Ifølge bemærkningerne til persondataloven anses Færøerne og Grønland ikke for dansk område efter be-

[27] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, pkt. 4.2.10.2 og 4.2.10.3 i de almindelige bemærkninger.

stemmelsen.[28] Det bemærkes dog, at persondataloven ved kongelig anordning nr. 1238 af 14. oktober 2016 er sat i kraft for Grønland den 1. december 2016.

Endvidere følger det af persondatalovens § 4, stk. 2, at loven gælder for den behandling, som udføres for danske diplomatiske repræsentationer.

Efter persondatalovens § 4, stk. 3, nr. 1, gælder loven også for en dataansvarlig, som er etableret i et tredjeland, hvis behandlingen af oplysninger sker under benyttelse af hjælpemidler, der befinder sig i Danmark, medmindre hjælpemidlerne kun benyttes med henblik på forsendelse af oplysninger gennem Det Europæiske Fællesskabs område.

Efter lovens § 4, stk. 4, er det et krav for dataansvarlige, som i henhold til stk. 3, nr. 1, er omfattet af persondataloven, at denne skal udpege en repræsentant, som er etableret i Danmark. Den registreredes mulighed for at foretage retslige skridt mod vedkommende dataansvarlige berøres efter bestemmelsen ikke heraf. Den dataansvarlige skal efter § 4, stk. 5, skriftligt underrette Datatilsynet om, hvem der er udpeget som repræsentant.

Efter persondatalovens § 4, stk. 3, nr. 2, gælder loven endvidere for en dataansvarlig, som er etableret i et tredjeland, hvis indsamling af oplysninger i Danmark sker med henblik på behandling i et tredjeland.

Desuden følger det af persondatalovens § 4, stk. 6, at loven gælder, hvis der for en dataansvarlig, der er etableret i et andet medlemsland, behandles oplysninger i Danmark, og behandlingen ikke er omfattet af databeskyttelsesdirektivet, ligesom det følger af bestemmelsen, at loven gælder, hvis der for en dataansvarlig, der er etableret i en stat, som har gennemført en aftale med Det Europæiske Fællesskab, der indeholder regler svarende til direktivet, behandles oplysninger i Danmark, og behandlingen ikke er omfattet af de nævnte regler.

Det bemærkes, at persondatalovens § 4, stk. 3, nr. 2, og § 4, stk. 6, går videre end forudsat i databeskyttelsesdirektivets artikel 4 om det territoriale anvendelsesområde. Der kan i den forbindelse bl.a. henvises til bemærkningerne til persondataloven og Registerudvalgets betænkning nr. 1345.[29]

[28] Bl.a. Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 4.
[29] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, pkt. 4.2.3.2 og 4.2.3.3 i de almindelige bemærkninger samt Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 217-224.

2.1.3. Databeskyttelsesforordningen

2.1.3.1. Materielt anvendelsesområde

2.1.3.1.1. Det almindelige anvendelsesområde

Databeskyttelsesforordningen gælder ifølge forordningens artikel 2, stk. 1, på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Begrebet "automatisk databehandling" er sammenfaldende med "edb" eller "elektronisk behandling", som anvendes i databeskyttelsesdirektivets artikel 3, stk. 1.

Bestemmelsen svarer således til det gældende databeskyttelsesdirektivs materielle anvendelsesområde.

2.1.3.1.2. Undtagelse af aktiviteter, der falder uden for EU-retten

Ifølge forordningens artikel 2, stk. 2, *litra a*, gælder forordningen ikke for behandling af personoplysninger under udøvelse af aktiviteter, der falder uden for EU-retten.

I forordningens præambelbetragtning nr. 16 er det anført, at der herved er tale om aktiviteter *såsom* aktiviteter vedrørende statens sikkerhed. Eksemplet om statens sikkerhed må på samme måde som eksemplerne i databeskyttelsesdirektivets artikel 3, stk. 2, 1. pind, umiddelbart antages at fastlægge rækkevidden af undtagelsen i litra a, således at den kun finder anvendelse på aktiviteter, der kan henføres til statens sikkerhed.

Baggrunden er, at forordningen har det samme grundlæggende formål som det gældende databeskyttelsesdirektiv samt i vidt omfang er en videreførelse og præcisering af direktivets regler.[30] Der må således skulle anlægges samme fortolkning af undtagelsen i forordningens artikel 2, stk. 2, som EU-Domstolen, som anført ovenfor under afsnit 2.1.2.2., anlagde i *Österreichischer Rundfunk*-sagerne og *Lindqvist*-sagen for databeskyttelsesdirektivets artikel 3, stk. 2, der ikke adskiller sig væsentligt fra undtagelserne i forordningen.

Således finder forordningen også anvendelse på aktiviteter, der konkret set ikke har et grænseoverskridende element. Det samme gør sig gældende på områder, der ikke som sådan hører under EU's kompetence. Forordningen finder derfor eksempelvis anvendelse i forbindelse med behandling af personoplysninger i sager om direkte beskatning, selvom

[30] Herved bl.a. forordningens artikel 1 og præambelbetragtning nr. 9-13 smh. databeskyttelsesdirektivets artikel 1 og præambelbetragtning nr. 8-10.

direkte beskatning ikke hører under EU's kompetence.[31] Det kan i den forbindelse tilføjes, at beskyttelse af personoplysninger i medfør af artikel 16 i TEUF er en del af EU-retten.

Ligesom persondataloven gælder forordningen derfor også for domstolene.

I modsætning til persondataloven må forordningen desuden antages at finde anvendelse for Folketinget og institutioner under Folketinget. For så vidt angår den behandling af personoplysninger, der foretages for Folketinget som led i det parlamentariske arbejde, herunder den betjening af Folketingets medlemmer, som Folketingets Administration foretager, må der imidlertid foretages en afgrænsning i forhold til informations- og ytringsfriheden, hvorom de nærmere grænser fastsættes ved lov, jf. forordningens artikel 85. For nærmere om artikel 85 henvises til afsnit 10.1. Den nærmere afgrænsning må i øvrigt udfyldes i praksis.

2.1.3.1.3. Undtagelse af aktiviteter i forbindelse med Unionens fælles udenrigs- og sikkerhedspolitik

Ifølge forordningens artikel 2, stk. 2, *litra b*, og præambelbetragtning nr. 16, gælder forordningen ikke for behandling af personoplysninger, som foretages af medlemsstaterne, når de udfører aktiviteter i forbindelse med Unionens fælles udenrigs- og sikkerhedspolitik (afsnit V, kapitel 2, i TEU).

Anvendelsesområdet for denne bestemmelse må, ligesom undtagelsen i artikel 2, stk. 2, litra a, antages at skulle fortolkes snævert.

2.1.3.1.4. Undtagelse af fysiske personers rent personlige eller familiemæssige aktiviteter

Ifølge forordningens artikel 2, stk. 2, *litra c*, gælder forordningen ikke for behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter.

2.1.3.1.5. Forholdet til retshåndhævelsesdirektivet

Ifølge forordningens artikel 2, stk. 2, *litra d*, gælder forordningen ikke for behandling af personoplysninger, som foretages af *kompetente myndigheder* med henblik på at forebygge, efterforske, afsløre eller retsforfølge *strafbare handlinger eller fuldbyrde strafferetlige sanktioner*, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

[31] Sag C-279/93, Schumacker, EU-Domstolens dom af 14. februar 1995, hvorefter medlemsstaterne skal overholde EU-retten, bl.a. bestemmelser om arbejdskraftens frie bevægelighed og forbuddet mod nationalitetsdiskrimination, når de udøver deres beskatningskompetence, selvom direkte beskatning er et område, der ikke som sådan hører under EU's kompetence.

Denne undtagelse vedrører ifølge præambelbetragtning nr. 19 forholdet til Europa-Parlamentets og Rådets direktiv (EU) 2016/680 (retshåndhævelsesdirektivet), som ifølge direktivets artikel 2, stk. 1, jf. § 1, stk. 1, finder anvendelse for sådanne behandlinger.

Retshåndhævelsesdirektivet er gennemført i dansk ret ved lov nr. 410 af 27. april 2017.

En *kompetent myndighed* defineres ifølge retshåndhævelsesdirektivets artikel 3, stk. 7, litra a, som enhver offentlig myndighed, der er kompetent med hensyn til at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

I Danmark er de kompetente myndigheder politiet, anklagemyndigheden, herunder den militære anklagemyndighed, kriminalforsorgen, Den Uafhængige Politiklagemyndighed og domstolene.

Ifølge direktivets artikel 3, nr. 7, litra b, er en kompetent myndighed endvidere ethvert andet organ eller enhver anden enhed, som i henhold til medlemsstaternes nationale ret udøver offentlig myndighed og offentlige beføjelser med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

I databeskyttelsesforordningens præambelbetragtning nr. 19 er det om forholdet til retshåndhævelsesdirektivet anført, at medlemsstater kan overdrage opgaver, der ikke nødvendigvis foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed, til de kompetente myndigheder som omhandlet i retshåndhævelsesdirektivet, således at behandling af personoplysninger til disse andre formål, for så vidt som de er omfattet af EU-retten, falder ind under databeskyttelsesforordningens anvendelsesområde.

Desuden er det anført, at medlemsstaterne med hensyn til disse kompetente myndigheders behandling af personoplysninger til formål, der er omfattet af anvendelsesområdet for denne forordning, bør kunne opretholde eller indføre mere specifikke bestemmelser for at tilpasse anvendelsen af reglerne i denne forordning. Sådanne bestemmelser kan mere præcist fastlægge specifikke krav til disse kompetente myndigheders behandling af personoplysninger til disse andre formål under hensyntagen til den forfatningsmæssige, organisatoriske og administrative struktur i den pågældende medlemsstat.

Når behandling af personoplysninger foretaget af private organer er omfattet af forordningens anvendelsesområde, bør forordningen give medlemsstaterne mulighed for på særlige betingelser ved lov at begrænse visse forpligtelser og rettigheder, når en sådan begrænsning udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund for at sikre bestemte vigtige interesser, herunder den offentlige sikkerhed og forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed. Dette er f.eks. relevant inden for rammerne af bekæmpelse af hvidvaskning af penge eller kriminaltekniske laboratoriers aktiviteter.

2.1.3.1.6. Forholdet til forordning (EF) nr. 45/2001

Det følger af forordningens artikel 2, stk. 3, at forordning (EF) nr. 45/2001 finder anvendelse på behandling af personoplysninger, som Unionens institutioner, organer, kontorer og agenturer foretager.

Endvidere følger det, at forordning (EF) nr. 45/2001 og andre EU-retsakter, der finder anvendelse på sådan behandling af personoplysninger, tilpasses til principperne og bestemmelserne i forordningen i overensstemmelse med artikel 98.

Kommissionen har den 12. januar 2017 fremsat forslag til revision af forordning nr. 45/2001 om EU's institutioner og organers behandling af personoplysninger. Formålet med forslaget er at tilpasse den gældende forordning med de principper og bestemmelser, der er fastsat i den generelle databeskyttelsesforordning, med henblik på at sikre en stærk og sammenhængende databeskyttelsesramme i EU, således at begge retsakter finder anvendelse samtidig. Forslaget viderefører de fleste elementer fra det gældende regelsæt. De væsentligste ændringer vedrører overordnet udvidelsen af reglerne for tilsynsmyndigheden og dennes sanktionsmuligheder, herunder muligheden for i visse tilfælde at pålægge EU-institutioner administrative bøder.

2.1.3.1.7. Forholdet til direktiv 2000/31/EF (e-handelsdirektivet)

Det følger af forordningens artikel 2, stk. 4, at forordningen ikke berører anvendelsen af direktiv 2000/31/EF, navnlig reglerne om formidleransvar for tjenesteydere, der er fastsat i artikel 12-15 i nævnte direktiv.

2.1.3.2. Territorialt anvendelsesområde

2.1.3.2.1. Dataansvarlig eller databehandler etableret i Unionen

Forordningen finder ifølge dennes artikel 3, stk. 1, anvendelse på behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en da-

tabehandler, som er *etableret* i Unionen, uanset om behandlingen finder sted i Unionen eller ej.

Begrebet "etableret" må antages at svare til begrebet som anvendt i databeskyttelsesdirektivets artikel 4, stk. 1, litra a. Ifølge EU-Domstolen omfatter begrebet enhver, selv minimal, reel og faktisk aktivitet, der udøves via en permanent struktur.

Bestemmelsen i artikel 3, stk. 1, adskiller sig på to punkter fra det gældende databeskyttelsesdirektivs territoriale anvendelsesområde, jf. direktivets artikel 4, stk. 1, litra a.

For det *første* sondrer bestemmelsen ikke, i modsætning til direktivets artikel 4, stk. 1, litra a, mellem de forskellige medlemsstater. Det afgørende er efter forordningens artikel 3, stk. 1, som anført, alene om den dataansvarlige eller databehandleren er etableret *i Unionen*.

Forordningens bestemmelser forholder sig ikke til valget mellem særreglerne i de forskellige medlemsstater vedtaget nationalt i overensstemmelse med forordningen, f.eks. artikel 6, stk. 2-3, og artikel 8, stk. 1. Det følger dog af databeskyttelsesforordningens præambelbetragtning nr. 153 om varierende nationale bestemmelser fastsat i medfør af forordningens artikel 85 om forholdet til ytrings- og informationsfriheden, at det er den nationale ret i den medlemsstat, den dataansvarlige er underlagt, som bør finde anvendelse. Et tilsvarende princip følger af det gældende databeskyttelsesdirektivs artikel 4, stk. 1, litra a, der bestemmer om forholdet mellem de forskellige medlemsstaters lovgivninger, som gennemfører direktivet, at det er lovgivningen i den medlemsstat eller de medlemsstater, hvor den dataansvarlige er *etableret*, der gælder for den dataansvarliges behandlingsaktiviteter.

Det vurderes, at ovennævnte tankegang i forordningens præambelbetragtning nr. 153 og det gældende databeskyttelsesdirektivs artikel 4, stk. 1, litra a, generelt kan udvides til også at finde anvendelse ved vurderingen af, hvilken medlemsstats nationale særregler, fastsat inden for rammerne af forordningen, der konkret finder anvendelse på en dataansvarligs behandlingsaktiviteter.

En medlemsstat må således antages at kunne bestemme, at forordningen og national lovgivning om behandling af personoplysninger, vedtaget inden for forordningens rammer, finder anvendelse på behandling, der foretages som led i aktiviteter inden for den medlemsstats område, hvor den dataansvarlige er etableret. På tilsvarende vis følger det som nævnt af persondatalovens § 4, stk. 1, at loven gælder for behandling af oplysninger, som udføres for en dataansvarlig, der er etableret i Danmark, hvis aktiviteterne finder sted inden for EU.

For det *andet* udvider forordningen det geografiske anvendelsesområde til at omfatte databehandlere, hvilket må antages at afspejle, at forordningen – i højere grad end det er tilfældet for databeskyttelsesdirektivet – indeholder specifikke regler vedrørende databehandleres behandling af personoplysninger.

2.1.3.2.2. Dataansvarlig og databehandler, der ikke er etableret i Unionen
Ifølge forordningens artikel 3, stk. 2, *litra a*, finder forordningen endvidere anvendelse på behandling af personoplysninger om registrerede, der er i Unionen, og som foretages af en dataansvarlig eller databehandler, der *ikke er etableret i Unionen*, hvis behandlingsaktiviteterne vedrører udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet.

Yderligere følger det af forordningens artikel 3, stk. 2, *litra b*, at forordningen finder anvendelse på behandling af personoplysninger om registrerede, der er i Unionen, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i Unionen, hvis behandlingsaktiviteterne vedrører overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Unionen.

Med forordningens artikel 3, stk. 2, ændres det territoriale anvendelsesområde i forhold til det gældende databeskyttelsesdirektivs område for dataansvarlige etableret i tredjelande. Bl.a. er det i forordningens artikel 3, stk. 2, litra a og b, ikke længere en betingelse, at behandlingen af oplysninger sker med hjælpemidler inden for EU. Dog vil hjælpemidler i EU formentlig i mange tilfælde kunne falde inden for anvendelsesområdet i medfør af forordningens artikel 3, stk. 1, idet der ifølge EU-Domstolens praksis ikke skal meget til, før en virksomhed mv. anses for etableret i Unionen.

Forordningens artikel 3, stk. 2, er udtryk for et virkningssynspunkt, som også kendes inden fra andre dele af EU-retten, f.eks. på varemærkeområdet, der går ud på, at forordningens skal finde anvendelse på behandlinger, der har virkning for fysiske personer, som befinder sig inden for EU's grænser.

Herudover er der en forskel i forhold persondatalovens § 4, stk. 3, nr. 2, hvorefter loven, som anført ovenfor i afsnit 2.1.2.8., gælder for dataansvarlige etableret i tredjelande, hvis indsamling af oplysningerne i Danmark sker med henblik på behandling i et tredjeland, idet forordningen ifølge artikel 3, stk. 2, kun gælder for en sådan behandling foretaget af en dataansvarlig eller databehandler i et tredjeland, i det omfang behandlingsaktiviteterne vedrører udbud af varer eller tjenester til registrerede i Unionen eller vedrører overvågning af registreredes adfærd, for så vidt deres adfærd finder sted i Unionen.

Endelig finder forordningen ifølge dennes artikel 3, stk. 3, anvendelse på behandling af personoplysninger, som foretages af en dataansvarlig, der ikke er etableret i Unionen, men et sted, hvor medlemsstaternes nationale ret gælder i medfør af folkeretten. Dette svarer til det gældende territoriale anvendelsesområde.

2.1.3.2.3. Forordningen i forhold til Færøerne og Grønland
I lyset af artikel 204 og artikel 355, stk. 5, litra a, i TEUF og protokol nr. 34 om den særlige ordning for Grønland, der er knyttet til Lissabontrakten, antages forordningen ikke at finde anvendelse for Færøerne og Grønland.

2.1.4. Overvejelser

2.1.4.1. Materielt anvendelsesområde
Det må antages, at forordningens almindelige anvendelsesområde svarer til persondatalovens § 1, stk. 1, dog med den forskel, at forordningen, modsat persondataloven, ikke uden videre finder anvendelse for personoplysninger om afdøde personer. Det er således præciseret i forordningens præambelbetragtning nr. 27, at medlemsstaterne kan fastsætte regler for behandling af personoplysninger om afdøde personer.

Det må samtidig antages, at det vil være muligt at videreføre persondatalovens § 1, stk. 1, i det omfang, det er nødvendigt af hensyn til sammenhængen og for at gøre nationale bestemmelser forståelige for de personer, som de finder anvendelse på, jf. herved bl.a. forordningens præambelbetragtning nr. 8. En sådan bestemmelse vil samtidig slå helt fast, at forordningen vil gælde på alle livsområder med undtagelse af statens sikkerhed og de øvrige områder, der er nævnt i forordningens artikel 3, stk. 2, litra b-d.

Persondatalovens øvrige anvendelsesområde, jf. lovens § 1, stk. 2-7, vedrører hovedsagligt forhold, som falder uden for forordningens anvendelsesområde, og forordningen vil således ikke være til hinder for, at der opretholdes sådanne tilsvarende regler inden for dette anvendelsesområde. Det samme gælder for persondatalovens § 1, stk. 8, om behandling af personoplysninger i forbindelse med tv-overvågning, i det omfang der er tale om brug af analogt tv-overvågningsudstyr.

Undtagelserne i persondatalovens § 2 vil overordnet ikke kunne opretholdes for så vidt angår forordningens almindelige anvendelsesområde, da undtagelserne i forordningens artikel 2, stk. 2, udtømmende gør op med undtagelserne fra anvendelsesområdet. Dog er der i forordningens artikel 85 regler om, at medlemsstaterne ved lov forener retten til beskyttelse af personoplysninger i henhold til forordningen med retten til ytrings- og informationsfrihed, herunder behandling i journalistisk øjemed og med henblik på akademisk, kunstnerisk eller litterær virksomhed.

Med forordningens artikel 2, stk. 2, litra a, videreføres en undtagelse svarende til undtagelsen i persondatalovens § 2, stk. 10, om behandlinger, der udføres for politiets og forsvarets efterretningstjenester.

Forordningens artikel 2, stk. 2, litra b, udvider undtagelsen i persondatalovens § 2, stk. 4, som kun undtager behandling af oplysninger på det strafferetlige område fra visse regler om de registrerede rettigheder. Efter forordningen falder det strafferetlige område helt uden for anvendelsesområdet. Til gengæld bliver området omfattet af retshåndhævelsesdirektivets anvendelsesområde.

Endelig viderefører forordningen en undtagelse svarende til undtagelsen i persondatalovens § 2, stk. 3, om behandling af personoplysninger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter, jf. forordningens artikel 2, stk. 2, litra c.

2.1.4.2. Territorialt anvendelsesområde

Forordningens territoriale anvendelsesområde er i vidt omfang det samme som i dag med den forskel, at forordningen gælder i alle medlemsstaterne til forskel fra de gældende nationale regler, der gennemfører databeskyttelsesdirektivet. Der er endvidere den forskel, at forordningens regler i videre omfang end regler fastsat på baggrund af direktivet også regulerer databehandleres behandling af personoplysninger mv. Desuden indskrænkes det geografiske anvendelsesområde som nævnt ovenfor i afsnit 2.1.2.8., i forhold til persondataloven for dataansvarlige etableret i tredjelande, når de indsamler oplysninger i Danmark med henblik på behandling i tredjeland, medmindre behandlingsaktiviteterne er omfattet af forordningens artikel 3, stk. 2, litra a eller b. I forhold til databeskyttelsesdirektivet kan forordningens artikel 3, stk. 2, litra a og b, imidlertid anses for en udvidelse af det geografiske anvendelsesområde, idet direktivet ikke – ligesom persondataloven – finder anvendelse for oplysninger indsamlet i Unionen med henblik på behandling i et tredjeland, og da der som anført ovenfor ikke skal meget til at anse benyttelsen af hjælpemidler i Unionen for etablering.

2.1.4.3. Forholdet til Færøerne og Grønland

Det bemærkes, at persondataloven, som anført ovenfor i afsnit 2.1.2.8., er sat i kraft for Grønland.

2.2. Rent privat karakter

2.2.1. Præsentation

Persondataloven gælder ikke for behandling af oplysninger, som en fysisk person foretager i forbindelse med aktiviteter af rent privat karakter. Baggrunden herfor er, at der i forbindelse med behandlinger af rent privat karakter ikke er samme beskyttelseshensyn at tage til den registrerede som med hensyn til f.eks. erhvervsvirksomheders behandling af personoplysninger i kommercielt øjemed.[32]

2.2.2. Gældende ret

Det følger af persondatalovens § 2, stk. 3, at loven ikke gælder for behandlinger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter.

Bestemmelsen bygger på artikel 3, stk. 2, 2. pind, i databeskyttelsesdirektivet, hvorefter direktivet ikke gælder for behandling af oplysninger, der foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter. Af præambelbetragtning nr. 12 til direktivet fremgår det, at en fysisk persons behandling af oplysninger som led i rent personlige eller familiemæssige aktiviteter, som f.eks. korrespondance og føring af en adressefortegnelse, ikke bør være omfattet af direktivet.

Det fremgår af bemærkningerne til persondatalovens § 2, stk. 3, at det at føre en elektronisk dagbog samt forskellige behandlinger i forbindelse med sædvanlige fritidsaktiviteter vil falde ind under bestemmelsen. Det nævnes endvidere, at den omstændighed, at en privatperson, f.eks. gennem internettet, giver et ubegrænset eller stort antal personer adgang til personoplysninger, ikke i sig selv vil være afgørende for, om behandlingen vil være omfattet af lovforslagets anvendelsesområde. Som eksempel nævnes, at det må antages, at deltagelse i debatter på internettet om sportsfolks præstationer mv. vil kunne være udtryk for aktiviteter af »rent privat karakter«.

Endvidere fremgår det, at udtrykket »rent privat karakter« således dækker over forskellige typer af behandlinger, som privatpersoner foretager i forbindelse med udøvelse af personlige eller familiemæssige aktiviteter.[33]

Bestemmelsen indebærer, at der skal være tale om sædvanlige og legitime private aktiviteter, således at bestemmelsen ikke anvendes til at omgå reglerne for lovlig behandling.[34] Endvidere vil behandling af oplysninger i forbindelse med erhvervsmæssige aktiviteter

[32] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 190.
[33] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 2.
[34] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 428.

ikke være omfattet af undtagelsen, og foreningsmæssige aktiviteter må som hovedregel antages heller ikke at være omfattet af undtagelsen i § 2, stk. 3. Herunder vil privatpersoners systematiske indsamling og registrering af oplysninger om andre personer vedrørende helbredsforhold, vaner og lignende næppe heller være undtaget fra reglerne i persondataloven, heller ikke selv om de er baseret på offentligt tilgængelige kilder.[35]

I sag C-101/01, Lindqvist, dom af 6. november 2003, udtalte EU-Domstolen vedrørende offentliggørelse af personoplysninger på en hjemmeside på internettet, at undtagelsen i databeskyttelsesdirektivets artikel 3, stk. 2, alene vedrører de aktiviteter, som indgår i den enkelte borgers privatliv eller familieliv, det vil sige ikke i forbindelse med behandling af personoplysninger, som består i, at oplysningerne offentliggøres på internettet for et ubestemt antal personer. Således konkluderede EU-Domstolen, at den omhandlede behandling ikke var omfattet af undtagelsen i artikel 3, stk. 2, 2. pind.

Vedrørende tv-overvågning udtalte Datatilsynet i notat af 13. september 2004 om tv-overvågning, at det er tilsynets umiddelbare opfattelse, at tv-overvågning, som en fysisk person foretager i sit eget hjem, er en aktivitet af rent privat karakter, og således falder uden for persondatalovens anvendelsesområde.[36]

I sag C-212/13, František Ryneš, dom af 11. december 2014, havde en privatperson anbragt et kamera på taget af den pågældendes familiebolig, som både filmede indgangen til huset, den offentlige vej og indgangen til genboens hus. Årsagen til installeringen af kameraet var, at personen ønskede at beskytte familiens ejendom, sundhed og liv, idet både personen og dennes familie igennem flere år havde været udsat for angreb fra en ukendt person. I den forbindelse udtalte EU-Domstolen, at undtagelsen i direktivets artikel 3, stk. 2, 2. led, skal undergives en streng fortolkning. Hvis en videoovervågning dækker et offentligt område – om end kun delvist – og derfor optager uden for det private rum, som den, der gennem overvågningen foretager behandlingen af disse oplysninger, befinder sig i, kan den ikke anses som en rent personlig eller familiemæssig aktivitet som omhandlet i direktivets artikel 3, stk. 2, 2. pind.

For så vidt angår sociale netværk har Artikel 29-gruppen udtalt, at det for behandling af personoplysninger på sådanne netværk som udgangspunkt gælder, at denne behandling er omfattet af undtagelsen i direktivets artikel 3, stk. 2, 2. pind. Artikel 29-gruppen har i den forbindelse udtalt, at såfremt en bruger handler på vegne af en forening, virksomhed mv.,

[35] Henrik Waaben og Kristian Korfits Nielsen, Lov om behandling af personoplysninger med kommentarer, 3. udgave (2015), s. 114-115 (herefter "Persondataloven med kommentarer (2015)").
[36] Notat af 13. september 2004 om tv-overvågning - Datatilsynets praksis og konkrete problemstillinger i forhold til gældende regulering på området af 13. september 2004, s. 8.

eller hvis formålet er kommercielt, politisk eller i forbindelse med velgørenhed, gælder undtagelsen ikke.

Det anføres endvidere i udtalelsen, at adgangen til oplysninger, som leveres af en bruger, typisk er begrænset til kontakter, som den pågældende selv har valgt. I nogle tilfælde kan brugere imidlertid erhverve et stort antal tredjepartskontakter, hvoraf der er nogle, som den pågældende rent faktisk ikke kender. Artikel 29-gruppen anfører, at et stort antal kontakter kunne være en indikation af, at undtagelsen ved udøvelse af familiemæssige aktiviteter ikke finder anvendelse.

Endvidere udtaler Artikel 29-gruppen, at når adgangen til profiloplysninger udvides til kontakter, som brugeren ikke selv har valgt, f.eks. når der gives adgang til en profil til samtlige medlemmer af det sociale netværk, eller når der ikke foretages nogen faktisk selektering med hensyn til godkendelse af kontakter, eller når dataene kan indekseres af søgemaskiner, går adgangen ud over de personlige og familiemæssige aktiviteter. Tilsvarende gælder, hvis en bruger træffer en informeret beslutning om at tillade adgang til ikke-selvvalgte "venner". Det er anført, at manglende adgangsbegrænsninger (og den deraf offentlige karakter) i flere medlemsstater betyder, at databeskyttelsesdirektivet finder anvendelse i relation til sådanne brugere.

Artikel 29-gruppen anfører endelig, at anvendelsen af undtagelsen ved udøvelse af familiemæssige aktiviteter ligeledes er begrænset af behovet for at garantere tredjeparters rettigheder, navnlig med hensyn til følsomme oplysninger.[37]

Der foreligger ikke praksis fra Datatilsynet, der kan bidrage til en mere præcis afgrænsning af udtrykket "aktiviteter af rent privat karakter" i forbindelse med behandling af personoplysninger på sociale netværk.

2.2.3. Databeskyttelsesforordningen

Det følger af databeskyttelsesforordningens artikel 2, stk. 2, litra c, at forordningen ikke gælder for behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter.

Det fremgår endvidere af præambelbetragtning nr. 18, at forordningen ikke gælder for en fysisk persons behandling af oplysninger under en rent personlig eller familiemæssig aktivitet og således uden forbindelse med en erhvervsmæssig eller kommerciel aktivitet. Personlige eller familiemæssige aktiviteter kan omfatte korrespondance og føring af en adres-

[37] Artikel 29-gruppens udtalelse nr. 5/2009 om internetbaserede sociale netværksaktiviteter (WP 163).

sefortegnelse eller sociale netværksaktiviteter og onlineaktiviteter, som udøves som led i sådanne aktiviteter.

Bestemmelsen i forordningens artikel 2, stk. 2, litra c, svarer efter ordlyden til bestemmelsen i databeskyttelsesdirektivets artikel 3, stk. 2, 2. pind, som er implementeret ved persondatalovens § 2, stk. 3.

Som udgangspunkt ses der således ikke at være tilsigtet ændringer i forhold til gældende ret.

Præambelbetragtning nr. 18 indeholder imidlertid i forhold til præambelbetragtning nr. 12 til direktivet den tilføjelse, at personlige eller familiemæssige aktiviteter kan omfatte sociale netværksaktiviteter og onlineaktiviteter, som udøves som led i sådanne aktiviteter.

Aktiviteter på sociale netværk var ikke aktuelle ved direktivets tilblivelse, og omtalen af onlineaktiviteter i øvrigt kan eventuelt ses som en justering af eller et supplement til EU-Domstolens afgørelse i Lindqvist-sagen.

Præambelbetragtning nr. 18 ses dog under alle omstændigheder at være i overensstemmelse med Artikel 29-gruppens udtalelse om internetbaserede sociale netværksaktiviteter.[38]

Tilføjelsen i præambelbetragtning nr. 18 udgør et vigtigt fortolkningsbidrag i forhold til fastlæggelsen af rækkevidden af begrebet "aktiviteter af rent privat karakter" ved behandling af personoplysninger på sociale netværk og andre onlineaktiviteter.

Det må derfor antages, at præambelbetragtning nr. 18 vil få væsentlig betydning for vurderingen i konkrete sager af rækkevidden af bestemmelsen i forordningens artikel 2, stk. 2, litra c.

Det kan herefter konkluderes, at forordningens artikel 2, stk. 2, litra c, er en videreførelse af de gældende regler med det fortolkningsbidrag, der følger af præambelbetragtning nr. 18.

2.2.4. Overvejelser

Som anført ovenfor er databeskyttelsesforordningens artikel 2, stk. 2, litra c, en videreførelse af reglerne i databeskyttelsesdirektivets artikel 3, stk. 2, 2. pind, og persondatalovens § 2, stk. 3, med det fortolkningsbidrag, der følger af præambelbetragtning nr. 18.

[38] Artikel 29-gruppens udtalelse nr. 5/2009 om internetbaserede sociale netværksaktiviteter (WP 163).

2.3. Definitioner, artikel 4

2.3.1. Præsentation

I artikel 4 i databeskyttelsesforordningen defineres en række af forordningens centrale begreber. Hvor databeskyttelsesdirektivet indeholder 8 definitioner, jf. direktivets artikel 2, litra a-h, indeholder forordningens artikel 4 hele 26 definitioner. En række af databeskyttelsesforordningens definitioner er nyskabelser; andre enten svarer til eller er ændrede i forhold til, hvad der følger af databeskyttelsesdirektivet. Definitionerne i databeskyttelsesdirektivets artikel 2, litra a-h, er gennemført i dansk ret ved persondatalovens § 3, nr. 1-8.

2.3.2. Gældende ret

Som nævnt ovenfor indeholder artikel 2, litra a-h, i databeskyttelsesdirektivet 8 legale definitioner. Der er tale om definitioner af begreberne *personoplysninger, behandling, register, registeransvarlig*, *registerfører*, *tredjemand, modtager* og *den registreredes samtykke.* Disse definitioner er alle gennemført i dansk ret ved persondatalovens § 3, nr. 1-8.

Af Registerudvalgets betænkning fremgår, at baggrunden for forslaget om at indføje alle databeskyttelsesdirektivets definitioner i persondataloven var at sikre, at der ikke kan rejses tvivl omkring gennemførelsen af bestemmelserne i direktivets artikel 2.[39] Det blev dog samtidig foreslået, at en række af definitionerne blev gjort kortere og mere præcise, end hvad der følger af direktivet. De eksemplifikationer, som er indeholdt i flere af direktivets definitioner, burde således efter Registerudvalgets opfattelse ikke indføjes i lovteksten, idet dette gik ud over overskueligheden. I stedet burde der tages højde for eksemplifikationerne i bemærkningerne til bestemmelserne. Registerudvalget foreslog endvidere, at der med hensyn til enkelte definitioner blev anvendt en anden terminologi, end hvad der følger af direktivet. I stedet for begreberne *den registeransvarlige* og *registerføreren* burde der således efter udvalgets opfattelse tales om *den dataansvarlige* og *databehandleren*. Der tilsigtedes herved ikke ændringer i forhold til indholdet af definitionerne i direktivet.

Herudover foreslog Registerudvalget, at der – foruden de definitioner, der var indeholdt i databeskyttelsesdirektivet – burde gives en legal definition af begrebet *tredjeland*.[40] Der blev herved lagt vægt på, at dette begreb – som en konsekvens af direktivet – vil skulle indarbejdes i visse af bestemmelserne i lovgivningen. Det gjaldt både i relation til reglerne om lovens geografiske område (§ 4), og for så vidt angår reglerne om overførsel af personoplysninger til tredjelande (§ 27). Der henvises i den forbindelse til persondatalovens § 3, nr. 9, og afsnit 2.3.2.8. nedenfor.

[39] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 209-210.
[40] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 217.

2.3.2.1. Begrebet "personoplysninger"

Ved *personoplysninger* forstås efter persondatalovens § 3, nr. 1, enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). Bestemmelsen har sin baggrund i artikel 2, litra a, i databeskyttelsesdirektivet.

Af bemærkningerne til persondatalovens § 3, nr. 1, fremgår det bl.a., at der ved udtrykket identificerbar person skal forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet.[41]

Omfattet af begrebet personoplysninger er ifølge bemærkningerne herefter oplysninger, som kan henføres til en fysisk person, selv om dette forudsætter kendskab til personnummer, registreringsnummer eller lignende særlige identifikationer som f.eks. løbenummer. Omfattet vil ligeledes bl.a. være oplysninger, som foreligger i form af billede, personens stemme, fingeraftryk eller genetiske kendetegn.

Det er uden betydning, hvorvidt identifikationsoplysningen er alment kendt eller umiddelbart tilgængelig, hvorfor også de tilfælde, hvor det kun for den indviede vil være muligt at forstå, hvem en oplysning vedrører, er omfattet af definitionen. Det er med andre ord ifølge bemærkningerne til bestemmelsen tilstrækkeligt, at der i forbindelse med behandlingen er etableret en ordning med et løbenummer eller lignende, f.eks. medlemsnummer eller journalnummer. Er f.eks. navn eller adresse erstattet af en kode, der kan føres tilbage til den oprindelige individuelle personoplysning, vil der stadigvæk være tale om en personoplysning.

Ved bedømmelsen af, om der er tale om personoplysninger i lovens forstand, vil det således principielt være uden betydning, på hvilken måde identifikationen kan foretages. En oplysning vil dermed falde ind under loven, selv om den først kombineret med andre oplysninger kan henføres til en fysisk person.

Ved afgørelsen af, om en person er identificerbar, skal alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende, enten af den dataansvarlige eller enhver anden person, tages i betragtning, jf. præambelbetragtning nr. 26 i databeskyttelsesdirektivet.

Det fremgår endvidere af bemærkningerne til persondatalovens § 3, nr. 1, at *krypterede oplysninger* også er omfattet, så længe nogen kan gøre oplysningerne læsbare og dermed

[41] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger § 3.

identificere de personer, som oplysningerne vedrører. Oplysninger, som er gjort *anonyme* på en sådan måde, at den registrerede ikke længere kan identificeres, er ikke omfattet af definitionen.

Af bemærkningerne til bestemmelsen fremgår endelig også, at elektronisk behandling af oplysninger om bestemte personer vil være omfattet af lovgivningen, uanset personerne kun er *bipersoner* i behandlingen.

Det fremgår af Registerudvalgets betænkning, at udvalget i forbindelse med fastlæggelsen af begrebet personoplysninger overvejede, om en dataansvarligs *subjektive vurderinger* af en fysisk person er at anse for en personoplysning i direktivets forstand.[42] Således som artikel 2, litra a, er affattet, syntes det efter udvalgets opfattelse uden betydning, hvorvidt oplysninger om en fysisk person er af objektiv eller subjektiv karakter. Afgørende er efter bestemmelsen, om der er tale om oplysninger, som kan henføres til en identificeret eller identificerbar person. Det kunne derfor efter udvalgets opfattelse næppe antages, at oplysninger om en fysisk person, som er af subjektiv karakter, falder uden for begrebet personoplysninger.

Bestemmelsen i direktivets artikel 15, stk. 1, synes ifølge udvalget også at forudsætte dette, idet bestemmelsen omfatter edb-behandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold, såsom erhvervsevne, kreditværdighed, pålidelighed, adfærd osv. I det omfang, der er tale om subjektive vurderinger af en fysisk person, f.eks. en læges diagnose af en patients psykiske helbredstilstand eller et pengeinstituts vurdering af en kundes kreditværdighed, må sådanne oplysninger derfor efter udvalgets opfattelse anses for omfattet af direktivets definition på personoplysninger.

Datatilsynets righoldige praksis i forhold til, hvornår der er tale om en personoplysning, er omtalt i persondataloven med kommentarer[43], hvoraf det tillige fremgår, at når definitionen af begrebet personoplysninger alene omfatter fysiske personer, indebærer det, at *virksomhedsoplysninger*[44], dvs. oplysninger om juridiske personer, såsom aktieselskaber, anpartsselskaber, kommanditselskaber, fonde, foreninger og visse selvejende institutioner mv., falder uden for lovens almindelige regulering, jf. persondatalovens § 1, stk. 1 og 2. Derimod er oplysninger om *enkeltmandsvirksomheder* omfattet, hvilket ligeledes må gælde virksomhedsoplysninger, der kan identificere enkeltpersoner, herunder f.eks. en oplysning om, at X er direktør i virksomheden Y. Mere tvivlsomt fremgår det at være, om oplysninger om *interessentskaber* skal antages at falde ind under lovens område, jf. § 1, stk. 1 og 2.

[42] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 211.
[43] Persondataloven med kommentarer (2015), s. 135 ff.
[44] Persondataloven med kommentarer (2015), s. 142.

Mest taler dog for – i det omfang interessenterne er fysiske personer – at ligestille oplysninger om interessentskaber med oplysninger om enkeltmandsvirksomheder og således anse sådanne oplysninger for at være omfattet af begrebet personoplysninger.

Persondataloven og dens forarbejderne forholder sig ikke til, om oplysninger om fostre er omfattet. I persondataloven med kommentarer antages det, at oplysninger om fostre – ligesom efter den hidtidige registerlovgivning – i almindelighed vil falde ind under begrebet personoplysninger. Der henvises i den forbindelse bl.a. til Registertilsynets j.nr. 1996-330-027 om Sundhedsstyrelsen (nu Sundhedsdatastyrelsens) misdannelsesregister, hvor der registreres visse oplysninger om fostre. Det fremgår endvidere, at det må være op til Datatilsynet i praksis at fastsætte, hvad det indebærer, at oplysninger om fostre falder ind under begrebet personoplysninger i forhold til bl.a. lovens bestemmelser om samtykke og den registreredes rettigheder.

Særligt for så vidt angår oplysninger om *afdøde* personer bemærkes, at det ikke fremgår udtrykkeligt af databeskyttelsesdirektivet, om oplysninger herom er at anse for personoplysninger. I Rådets mødeprotokol vedrørende direktivet har Rådet og EU-Kommissionen imidlertid i erklæring nr. 5 bekræftet, at det er overladt til medlemsstaterne at beslutte, i hvilken udstrækning direktivet finder anvendelse på oplysninger om afdøde personer.

I bemærkningerne til persondatalovens § 3, nr. 1, og navnlig under pkt. 4.2.2.3. i lovforslagets almindelige bemærkninger, lægges der med hensyn til oplysninger om afdøde personer derfor op til, at sådanne oplysninger i samme udstrækning som efter den tidligere gældende retstilstand skal anses for personoplysninger og dermed være omfattet af lovens regulering. Dette indebærer, at allerede behandlede oplysninger, f.eks. registrerede oplysninger, efter personens død fortsat vil være omfattet af loven – i hvert fald i en vis tid. Det vil også indebære, at indsamling og efterfølgende behandling af oplysninger om afdøde personer skal opfylde lovens betingelser, hvis der foreligger et særligt beskyttelsesbehov, hvilket i praksis navnlig vil få betydning for behandling af følsomme oplysninger om afdøde personer. Til eksempel på et register, der behandler oplysninger om afdøde personer, og som er reguleret af persondataloven, kan nævnes Dødsårsagsregisteret, der føres af Sundhedsdatastyrelsen. I registret registreres bl.a. oplysninger om dødsårsager, køn og alder på dødstidspunkt. Det er dog samtidig klart, at en række af lovens regler i sagens natur ikke kan finde anvendelse i forbindelse med behandling af oplysninger om afdøde personer. Det gælder f.eks. regler, der forudsætter den registreredes samtykke, og reglerne om oplysningspligt over for den registrerede i lovens kapitel 8. I lovens forarbejder er det forudsat, at de problemer, der herved måtte opstå, i praksis løses gennem tilsynsmyndighedernes anvendelse af loven.

Et spørgsmål, der flere gange har været berørt af Artikel 29-gruppen, er spørgsmålet om, hvorvidt der behandles personoplysninger i forbindelse med brug af cookies og adfærdsbaseret annoncering.[45]

Artikel 29-gruppen har i den forbindelse bl.a. udtalt, at de metoder til adfærdsbaseret annoncering, der er beskrevet i deres udtalelse, ofte medfører behandling af personoplysninger som defineret i artikel 2 i databeskyttelsesdirektivet og fortolket af Artikel 29-gruppen. Dette skyldes, ifølge Artikel 29-gruppen, flere ting: i) Adfærdsbaseret annoncering omfatter normalt indsamling af IP-adresser og behandling af unikke identifikatorer (via cookien). Artikel 29-gruppen anfører endvidere, at brugen af sådanne anordninger med en unik identifikator gør det muligt at spore brugerne af en bestemt computer, selv om der anvendes dynamiske IP-adresser. Det fremgår endvidere af Artikel 29-gruppens udtalelser, at sådanne anordninger med andre ord gør det muligt at "udpege" registrerede, selv om deres virkelige navne ikke kendes. ii) De oplysninger, der indsamles i forbindelse med adfærdsbaseret annoncering vedrører (dvs. handler om) en persons egenskaber eller adfærd, og de bruges til at påvirke lige netop den pågældende person. Artikel 29-gruppen anfører endvidere, at denne holdning bekræftes yderligere, hvis muligheden for, at profiler på ethvert tidspunkt kan kædes sammen med direkte personligt identificerbare oplysninger, som den registrerede har angivet, f.eks. registreringsrelaterede oplysninger, tages i betragtning. Endelig anfører Artikel 29-gruppen i deres udtalelser, at andre scenarier, der kan føre til identificerbarhed, er datafletning, datatab og den øgede tilgængelighed af personoplysninger på internettet i kombination med IP-adresser.

I sag C-582/14, Patrick Breyer, dom af 19. oktober 2016, blev EU-Domstolen forelagt et præjudicielt spørgsmål af en tysk domstol om, hvorvidt en dynamisk IP-adresse udgør personoplysninger efter databeskyttelsesdirektivets artikel 2, litra a. EU-domstolen udtalte, at bestemmelsen i direktivet skal fortolkes således, at en dynamisk IP-adresse, som en udbyder af online-medietjenester registrerer i forbindelse med en søgning foretaget af en person på en internetside, som denne udbyder gør tilgængelig for offentligheden, i forhold til den nævnte udbyder udgør en personoplysning som omhandlet i databeskyttelsesdirektivets artikel 2, litra a, når udbyderen råder over lovlige hjælpemidler, der gør det muligt for denne at få identificeret den registrerede gennem den yderligere viden, som denne persons internetudbyder råder over.

I lighed med ovennævnte, er et andet vigtigt spørgsmål, hvornår biologisk materiale er at betragte som personoplysninger. Dette er tilfældet, når oplysningerne, der er bundet i det biologiske materiale, kan henføres til enkeltpersoner. Ved afgørelsen af, om biologisk ma-

[45] Bl.a. Artikel 29-gruppens udtalelser nr. 1/2008 om databeskyttelsesproblemer i forbindelse med søgemaskine (WP 148) og nr. 2/2010 om adfærdsbaseret annoncering på internettet (WP 171).

teriale *i sig selv* udgør en personoplysning, skal alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende, enten af den dataansvarlige eller enhver anden person, tages i betragtning. Hvis man gennemfører en omfattende sekventering af en persons arvemasse (whole genome sequenzing) og andre analyser på baggrund af f.eks. en blodprøve, vil man kunne tilvejebringe flere oplysninger af varierende brugbarhed for identifikation. Denne mulighed vil løbende udvides i takt med, at man f.eks. bliver bedre til at analysere biologisk materiale, at sådanne analyser bliver billigere, at man bliver bedre til at koble resultaterne herfra med andre tilgængelige datasæt og oplysninger (f.eks. oplysninger fra sociale medier, etc.), og at data opbevares længere og i højere grad udbredes. Hvis der f.eks. ligger genomoplysninger på personen selv eller vedkommendes slægtninge i andre databaser (f.eks. slægtsskabsdatabaser eller i forskningsdatabaser med tilknyttede oplysninger i form af køn, alder eller ligefrem personnummer, etc.), stiger mulighederne for at kunne identificere en person ud fra det pågældende biologiske materiale.

Endelig har Artikel 29-gruppen i en udtalelse af 20. juni 2007[46] mere generelt udtalt sig om, hvornår en oplysning er en personoplysning i direktivets forstand. I udtalelsen gives der en række konkrete eksempler på, hvornår en given oplysning må betragtes som en personoplysning.

2.3.2.2. Begrebet "behandling"

Efter persondatalovens § 3, nr. 2, forstås ved *behandling* enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for. Bestemmelsen har sin baggrund i artikel 2, litra b, i databeskyttelsesdirektivet.

Af bemærkningerne til persondatalovens § 3, nr. 2, fremgår det bl.a., at bestemmelsen er en nyskabelse i forhold til den gældende registerlovgivning, da begrebet, ud over registrering, opbevaring og videregivelse af oplysninger, omfatter enhver form for håndtering af oplysninger.[47] Begrebet dækker således bl.a. over indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden overladelse, sammenstilling eller samkøring samt blokering, sletning eller tilintetgørelse. Finder blot en af de nævnte former for håndtering af oplysninger sted, vil der være tale om behandling i bestemmelsens forstand.

I persondataloven med kommentarer gennemgås en række situationer – bl.a. med udgangspunkt i Datatilsynets praksis – med henblik på at fastslå, om der er tale om en behandling i

[46] Artikel 29-gruppens udtalelse nr. 4/2007 om begrebet personoplysninger (WP 136).
[47] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.

persondatalovens forstand.[48] Endvidere gennemgås en række af de behandlingsformer, der er nævnt ovenfor nærmere. Det gælder bl.a. sondringen mellem *videregivelse* og *overladelse* af personoplysninger.[49] I den sammenhæng nævnes det, at en dataansvarligs overladelse af personoplysninger til en databehandler (f.eks. et edb-servicebureau) ikke i sig selv kan anses for at være en behandling i § 3, nr. 2's forstand med den virkning, at sådan overladelse alene kan finde sted under iagttagelse af behandlingsreglerne i persondatalovens kapitel 4. Det bør derimod være muligt for en dataansvarlig uafhængigt af behandlingsreglerne i kapitel 4 at beslutte sig for at benytte en databehandler til den tekniske bearbejdning af personoplysninger, naturligvis under fuldstændig iagttagelse af kravene til datasikkerhed, jf. lovens kapitel 11. Samme sted nævnes det, at formentlig også andre former for overladelser (end med henblik på ren teknisk forarbejdning) må betragtes således, at der ikke i sig selv er tale om en behandling i § 3, nr. 2's forstand. Som eksempler herpå nævnes overladelser til f.eks. advokater og revisorer med henblik på rådgivning om et spørgsmål.

2.3.2.3. Begrebet "register med personoplysninger" ("register")

Af persondatalovens § 3, nr. 3, fremgår det, at et *register* er enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grundlag. Bestemmelsen har sin baggrund i artikel 2, litra c, i databeskyttelsesdirektivet.

Det fremgår af bemærkningerne til persondatalovens § 3, nr. 3[50], at bestemmelsens registerbegreb omfatter manuelle registre, såsom fortegnelser, kartotekskasser, journalsystemer og andre samlinger af manuelt materiale, som opbevares struktureret efter bestemte kriterier vedrørende personer for at lette adgangen til de indeholdte personoplysninger. Derimod er manuelle akter, som indgår i den dataansvarliges konkrete sagsbehandling, mapper med sagsakter eller samlinger af sådanne mapper ikke omfattet af registerbegrebet. Endelig fremgår det, at den nærmere afgrænsning af registerbegrebet må finde sted gennem Datatilsynets praksis.

2.3.2.4. Begrebet "den dataansvarlige"

Ved *den dataansvarlige* forstås efter persondatalovens § 3, nr. 4, den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. Bestemmelsen bygger på artikel 2, litra d, i databeskyttelsesdirektivet.

[48] Persondataloven med kommentarer (2015), s. 145 ff.
[49] Persondataloven med kommentarer (2015), s. 149 og s. 154-156.
[50] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.

Af bemærkningerne til persondatalovens § 3, nr. 4[51], fremgår det, at begrebet ikke er defineret i registerlovgivningen, men at definitionen må antages at svare til, hvad der i dag antages at gælde på ulovbestemt grundlag.

Artikel 29-gruppen har i en udtalelse af 16. februar 2010[52] udtalt sig om begreberne *den registeransvarlige* og *registerføreren* samt givet en række eksempler på, hvornår en virksomhed eller et organ må være at betragte som henholdsvis registeransvarlig (dataansvarlig) og registerfører (databehandler).

Af udtalelsen fremgår bl.a., at begrebet den dataansvarlige og dets samspil med begrebet databehandler spiller en afgørende rolle for anvendelsen databeskyttelsesdirektivet, da disse to begreber fastlægger, hvem der er ansvarlig for overholdelsen af databeskyttelsesregler, hvordan de registrerede kan udøve deres rettigheder, hvilken national lov der skal anvendes, og hvordan effektive databeskyttelsesmyndigheder kan fungere.

Organisatorisk differentiering i både den offentlige og den private sektor, udviklingen af informations- og kommunikationsteknologi samt globaliseringen af databehandling øger kompleksiteten af den måde, som personoplysninger behandles på, og kræver en afklaring af disse begreber for at sikre en effektiv anvendelse og overholdelse i praksis.

Endvidere fremgår det, at begrebet den dataansvarlige, efter Artikel 29-gruppens opfattelse, er selvstændigt i den forstand, at det primært skal fortolkes i overensstemmelse med fællesskabslovgivningen om databeskyttelse og funktionelt i den forstand, at det skal tildele ansvarsområder i forhold til den faktiske indflydelse, og det er således snarere baseret på en faktuel end en formel analyse.

Artikel 29-gruppen udtaler endvidere, at definitionen i databeskyttelsesdirektivet indeholder tre primære byggesten: 1) Det personlige aspekt ("den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ"), 2) muligheden for pluralistisk kontrol ("der alene eller sammen med andre") og 3) de væsentlige elementer, der adskiller den dataansvarlige fra andre aktører ("afgør, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger").

Analysen af disse elementer fører, ifølge Artikel 29-gruppen, til hovedresultatet, at evnen til at "afgøre, til hvilket formål og med hvilke hjælpemidler […]" kan stamme fra forskellige juridiske og/eller faktiske omstændigheder: En eksplicit juridisk kompetence, når loven udnævner den dataansvarlige eller pålægger en opgave eller pligt til at indsamle og be-

[51] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.
[52] Artikel 29-gruppens udtalelse nr. 1/2010 om begreberne "registeransvarlig" og "registerfører" (WP 169).

handle bestemte oplysninger, almindelige juridiske bestemmelser eller eksisterende traditionelle roller, der normalt omfatter et bestemt ansvar inden for visse organisationer (f.eks. arbejdsgiveren i forhold til oplysninger om dennes medarbejdere), faktiske omstændigheder og andre elementer (som f.eks. kontraktforhold, en parts faktiske kontrol, synlighed over for de registrerede osv.).

Artikel 29-gruppen udtaler, at hvis ingen af disse kategorier er relevante, skal udnævnelsen af en dataansvarlig anses for at være "ugyldig". Et organ, som hverken har juridisk eller faktisk indflydelse på at afgøre, hvordan personoplysninger behandles, kan, ifølge Artikel 29-gruppen, ikke anses for at være den dataansvarlige.

Artikel 29-gruppen anfører endvidere, at fastlæggelsen af "formålet" med en behandling udløser kvalificeringen som (reelt) dataansvarlig. Derimod kan fastlæggelsen af "hjælpemidlerne" ved en behandling, ifølge Artikel 29-gruppen, uddelegeres af den dataansvarlige, for så vidt angår tekniske eller organisatoriske spørgsmål. Artikel 29-gruppen udtaler endvidere, at væsentlige spørgsmål, som er afgørende for lovligheden af en behandling – som f.eks. de oplysninger, der skal behandles, opbevaringsperioden, adgang osv. –dog skal fastlægges af den dataansvarlige.

Herudover udtaler Artikel 29-gruppen, at det personlige aspekt af definitionen henviser til en lang række aktører, som kan udfylde funktionen som den dataansvarlige. Med henblik på en strategisk tildeling af ansvar bør det dog, ifølge Artikel 29-gruppen, foretrækkes at anse selve virksomheden eller organet som den dataansvarlige snarere end en bestemt person i virksomheden eller organet. Ifølge Artikel 29-gruppen er det virksomheden eller organet, som i sidste instans anses for at være ansvarlig for databehandlingen og de forpligtelser, der er baseret på databeskyttelseslovgivningen, medmindre der er klare elementer, som indikerer, at en fysisk person er ansvarlig, f.eks. når en fysisk person, der arbejder i en virksomhed eller et offentligt organ, anvender oplysninger til sine egne formål uden for virksomhedens aktiviteter.

Artikel 29-gruppen udtaler endvidere, at muligheden for pluralistisk kontrol (delt dataansvar) imødekommer det stigende antal situationer, hvor forskellige parter handler som dataansvarlige. Vurderingen af denne fælles kontrol skal, ifølge Artikel 29-gruppen, afspejle vurderingen af den "enkelte" kontrol, ved at der anlægges en selvstændig og funktionel tilgang, idet der fokuseres på, hvorvidt formålene og de væsentlige elementer ved hjælpemidlerne fastlægges af mere end én part.

Af nyere retspraksis fra EU-Domstolen vedrørende begrebet dataansvarlig kan nævnes Google Spain SL og Google Inc., sag nr. C-131/12. I denne dom fastslår domstolen bl.a., at

udbyderen af en søgemaskine skal anses for dataansvarlig for den behandling af personoplysninger, der finder sted i forbindelse med søgemaskinens aktiviteter, der består i at finde oplysninger, der er offentliggjort eller lagt på internettet af tredjemand, indeksere disse automatisk, lagre dem midlertidigt og sluttelig gøre dem tilgængelige for internetbrugerne i en vis prioriteret orden.

2.3.2.5. Begrebet "databehandleren"

Efter persondatalovens § 3, nr. 5, forstås ved *databehandleren* den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne. Bestemmelsen har sin baggrund i artikel 2, litra e, i databeskyttelsesdirektivet.

Af bemærkningerne til persondatalovens § 3, nr. 5[53], fremgår det – i lighed med hvad der var tilfældet i forhold til *den dataansvarlige* – at begrebet databehandleren ikke er defineret i registerlovene, men at begrebet må antages at svare til, hvad der efter gældende registerlovgivning anses for en databehandler.

Som nævnt ovenfor har Artikel 29-gruppen i en udtalelse af 16. februar 2010 udtalt sig om begreberne *dataansvarlig* og *databehandler*.

I udtalelsen anfører Artikel 29-gruppen bl.a. om begrebet registerfører (databehandler), at dennes eksistens afhænger af den registeransvarlige (dataansvarlige), som kan beslutte enten at behandle oplysninger i sin egen organisation eller at uddelegere alle eller en del af behandlingsaktiviteterne til en ekstern organisation. Derfor findes der, ifølge Artikel 29-gruppen, to grundlæggende betingelser for at være kvalificeret som databehandler: På den ene side skal der være tale om en retligt selvstændig enhed i forhold til den dataansvarlige, og på den anden side skal databehandleren behandle personoplysninger på den dataansvarliges vegne. Artikel 29-gruppen udtaler endvidere, at denne behandlingsaktivitet kan være begrænset til en meget specifik opgave eller sammenhæng eller omfatte en vis grad af frihed i forhold til at opfylde den dataansvarliges interesser, hvilket giver databehandleren mulighed for at vælge de mest velegnede tekniske og organisatoriske hjælpemidler.

Artikel 29-gruppen bemærker desuden, at rollen som databehandler ikke stammer fra karakteren af en aktør, der behandler personoplysninger, men fra dennes konkrete aktiviteter i en bestemt sammenhæng og med hensyn til en bestemt række oplysninger eller operationer. Nogle kriterier kan, ifølge Artikel 29-gruppen, bidrage til at fastlægge kvalifikationerne hos de forskellige aktører, der er involveret i behandlingen: niveauet af forudgående

[53] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.

instrukser fra den dataansvarlige, den dataansvarliges overvågning af niveauet af ydelsen, synligheden over for de registrerede, parternes ekspertise, de forskellige parters beføjelser til at træffe selvstændige beslutninger.

Ved siden af ovennævnte generelle betragtninger giver Artikel 29-gruppen i sin udtalelse også en række konkrete eksempler på situationer, hvor en virksomhed eller et organ fungerer som databehandler, herunder f.eks. hvornår en revisor eller en advokat må betragtes som databehandler.

Herudover fremgår det af persondataloven med kommentarer[54], at ved begrebet databehandler er det centrale, at databehandleren behandler oplysninger på den dataansvarliges vegne, således at det er den dataansvarlige og ikke databehandleren, der er direkte ansvarlig over for den registrerede. Det skal med andre ord være en forudsætning mellem parterne, at den private virksomhed mv. uden for den dataansvarliges organisation, der modtager oplysningerne, ikke selv kan disponere over oplysningerne til egne formål eller i øvrigt uden den dataansvarliges accept.

En databehandler vil sædvanligvis være en privat erhvervsvirksomhed, men kan principielt også være en fysisk person, offentlig myndighed, institution mv., når bare organets behandling af oplysninger sker på den dataansvarliges vegne. I persondataloven med kommentarer[55] er opregnet en række eksempler på, hvornår der er tale om en databehandler. Det drejer sig blandt andet om edb-servicebureauer, internethoteller, outsourcing og med hensyn til facility management virksomheder. Endvidere kan nævnes konsulentfirmaer, der indsamler og bearbejder personoplysninger i forbindelse med udførelsen af en opgave på den dataansvarliges vegne samt – efter omstændighederne – en advokat eller en revisor, som behandler oplysninger med henblik på at rådgive den dataansvarlige om et givent spørgsmål.

Det bemærkes i den forbindelse, at hvis det er en forudsætning mellem parterne, at den oprindelige dataansvarlige ikke længere har rådighed over oplysningerne, og at den modtagende part kan anvende oplysningerne til egne formål, er dataansvaret overgået til den modtagende part, der betragtes som tredjemand og ny dataansvarlig. En sådan behandling af oplysninger betegnes som en videregivelse.

2.3.2.6. Begrebet "tredjemand"

I persondatalovens § 3, nr. 6, defineres en *tredjemand* som enhver anden fysisk eller juridisk person, offentlig myndighed, institution eller ethvert andet organ end den registrerede,

[54] Persondataloven med kommentarer (2015), s. 165.
[55] Persondataloven med kommentarer (2015), s. 165-166.

den dataansvarlige, databehandleren og de personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle oplysninger. Bestemmelsen har sin baggrund i artikel 2, litra f, i databeskyttelsesdirektivet.

Det fremgår af bemærkningerne til persondatalovens § 3, nr. 6, at bestemmelsen er en nyskabelse i forhold til den gældende registerlovgivning. Endvidere fremgår det, at begrebet tredjemand bl.a. har betydning med hensyn til spørgsmålet om den dataansvarliges adgang til at behandle, herunder videregive, oplysninger, jf. § 6, nr. 6 og 7, og om den dataansvarliges pligt til at underrette tredjemand om berigtigelse, sletning eller blokering af videregivne oplysninger, jf. § 37, stk. 2.

2.3.2.7. Begrebet "modtager"

Ved begrebet *modtager* forstås efter persondatalovens § 3, nr. 7, den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, hvortil oplysningerne meddeles, uanset om der er tale om en tredjemand. Myndigheder, som vil kunne få meddelt oplysninger som led i en isoleret forespørgsel betragtes ikke som modtagere. Bestemmelsen svarer til artikel 2, litra g, i databeskyttelsesdirektivet.

Af bemærkningerne til persondatalovens § 3, fremgår det bl.a., at definitionen har betydning i relation til reglerne om henholdsvis den dataansvarliges oplysningspligt og den registreredes indsigtsret, jf. persondatalovens § 28, stk. 1, nr. 3, litra a, § 29, stk. 1, nr. 3, litra b, og § 31, stk. 1, nr. 3. Begrebet er endvidere af betydning i relation til reglerne om anmeldelse af behandlinger, jf. § 43, stk. 2, nr. 5, § 48, stk. 2, og § 52.

Det fremgår af bestemmelsen, at principielt enhver, som modtager oplysninger fra den dataansvarlige, er en modtager. I persondataloven med kommentarer anføres det[56], at det ikke kan være tilsigtet med bestemmelsen. Omfattet af bestemmelsen er ifølge forfatterne med sikkerhed tredjemænd som angivet i persondatalovens § 3, nr. 6, men også edb-servicebureauer og andre databehandlere må anses for omfattet af modtagerbegrebet. Derimod kan afdelinger, kontorer eller en lignende del af selve den dataansvarliges organisation ikke antages at være modtagere i lovens forstand. Der henvises i den forbindelse til Domstolsstyrelsens generelle vejledning om persondataloven (februar 2006) pkt. 3.3, hvor det anføres, at begrebet modtager ikke omfatter enheder inden for den dataansvarlige ret. Hvis oplysninger f.eks. overføres fra fogedretten til skifteretten ved samme embede, er skifteretten ikke modtager. Lægdommere, der modtager oplysninger om en konkret sag med henblik på at dømme i sagen, er heller ikke omfattet. Derimod er f.eks. stævningsmænd, politiet, kuratorer, bobestyrere, revisorer, sagkyndige eller andre, der modtager op-

[56] Persondataloven med kommentarer (2015), s. 167.

lysninger med henblik på at udføre en opgave for den dataansvarlige ret, parter i en sag og andre offentlige myndigheder ifølge vejledningen at anse for omfattet af modtagerbegrebet.

Som det er tilfældet mellem enheder inden for den samme dataansvarlige ret, vil forvaltninger, afdelinger mv. heller ikke være at betragte som modtagere i lovens forstand, når der overføres oplysninger inden for den kommunale enhedsforvaltning.[57]

2.3.2.8. Begrebet "samtykke"

Den registreredes *samtykke* defineres i persondatalovens § 3, nr. 8, som enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling. Bestemmelsen er formuleret under hensyn til, hvad der ifølge artikel 2, litra h, i databeskyttelsesdirektivet forstås ved begrebet samtykke.

Det fremgår af bemærkningerne til persondatalovens § 3, nr. 8[58], at et samtykke skal meddeles i form af en viljestilkendegivelse fra den registrerede. Heraf følger, at et samtykke som udgangspunkt skal meddeles af den registrerede selv. Der er dog ikke noget til hinder for, at et samtykke meddeles af en person, som af den registrerede er meddelt fuldmagt hertil.

Herudover fremgår det af bemærkningerne, at der ikke gælder noget formkrav til et samtykke, som således både kan være skriftligt og mundtligt. Da bevisbyrden for, at der foreligger et samtykke, der opfylder lovens krav, påhviler den dataansvarlige, må det dog anbefales, at et samtykke i videst muligt omfang afgives skriftligt. Dette vil ifølge bemærkningerne navnlig gælde, hvis der afgives samtykke til behandling af oplysninger, som er af følsom karakter, eller hvis samtykket i øvrigt har stor betydning for en eller flere af parterne. Et samtykke skal endvidere være frivilligt. Samtykket må således ikke være afgivet under tvang. Dette gælder, uanset om det er den dataansvarlige selv eller andre, der øver pression over for den registrerede.

I kravet om, at der skal være tale om et specifikt samtykke, ligger ifølge bemærkningerne til bestemmelsen, at samtykket skal være konkretiseret i den forstand, at det klart og utvetydigt fremgår, hvad der meddeles samtykke til. Det skal således af et meddelt samtykke fremgå, hvilke typer af oplysningerne der må behandles, hvem der kan foretage behandling af oplysninger om den samtykkende, og til hvilke formål behandlingen kan ske.

[57] Se mere om den kommunale enhedsforvaltning i Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave (2013), s. 394 ff.
[58] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.

Endelig skal samtykket ifølge bemærkningerne til bestemmelsen være informeret i den forstand, at den samtykkende skal være klar over, hvad det er, vedkommende meddeler samtykke til. Den dataansvarlige må således sikre sig, at den registrerede gives tilstrækkelig information til, at den pågældende kan vurdere, hvorvidt samtykke bør meddeles.

Af bemærkningerne til bestemmelsen fremgår endvidere, at den registrerede på et hvilket som helst tidspunkt kan tilbagekalde et samtykke, jf. lovens § 38. Virkningen heraf vil i givet fald være, at den behandling af oplysninger, som den registrerede tidligere har meddelt sit samtykke til, ikke længere må finde sted. Den registrerede kan derimod ikke tilbagekalde sit samtykke med tilbagevirkende kraft.

Af Registerudvalgets betænkning nr. 1345 fremgår det tillige[59], at der med databeskyttelsesdirektivets formuleringer – i f.eks. artikel 7, litra a og artikel 26, stk. 1, litra a – om, "at der ikke må herske tvivl om, at den registrerede har givet sit samtykke" formentlig må antages at ligge et krav om, at et samtykke skal være klart og utvetydigt. Endvidere må udtrykket "udtrykkeligt" i databeskyttelsesdirektivets artikel 8, stk. 2, litra a, efter udvalgets opfattelse antages at føre til, at der ikke er mulighed for, at den dataansvarlige opnår stiltiende eller indirekte tilslutning fra den registrerede.

I forhold til *børns samtykke* fremgår det af persondataloven med kommentarer[60], at det må antages, at forældre til mindreårige børn i almindelighed kan meddele samtykke på vegne af deres børn, idet det dog konkret må vurderes, om dette i forhold til bl.a. oplysningernes karakter bør accepteres. Med hensyn til om mindreårige på egen hånd kan meddele samtykke til behandling af personoplysninger, fremgår det af forvaltningsloven med kommentarer[61], at bl.a. i situationer, hvor den mindreårige – efter lovgivningen – selv kan starte en ansøgningssag, må vedkommende også selv kunne give samtykke til indhentelse af oplysninger efter forvaltningslovens § 29. Hvis lovgivningen ikke indeholder regler eller forudsætninger om, at den mindreårige kan optræde på egen hånd, må det antages, at den mindreårige selv kan meddele samtykke, hvis den unge har den modenhed, som på det givne sagsområde er nødvendigt for at forstå og overse konsekvenserne af samtykket, og der er grund til at antage, at der foreligger stiltiende samtykke fra forældremyndighedsindehaveren, eller at denne ikke vil modsætte sig samtykket.

Om kravet om, at et samtykke skal være frivilligt, fremgår det af persondataloven med kommentarer[62] bl.a., at der i praksis vil kunne forekomme situationer, hvor der kan rejses

[59] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 215 ff.
[60] Persondataloven med kommentarer (2015), s.168 ff.
[61] Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave (2013), s. 832 ff.
[62] Persondataloven med kommentarer (2015), s. 171 f.

spørgsmål om, hvorvidt et samtykke er frivilligt. Der peges i den forbindelse f.eks. på den situation, hvor den registrerede opnår en modydelse for at meddele samtykke.

For så vidt angår kravet om at et samtykke skal være informeret, fremgår det af persondataloven med kommentarer[63], at der heri må ligge, at den dataansvarlige skal oplyse sin identitet, formålet med behandlingen og hvilke former for behandlinger der påtænkes, herunder i hvilken udstrækning videregivelse vil ske.

Særligt i forhold til såkaldt *formidlet samtykke* fremgår det af persondataloven med kommentarer[64], at persondataloven ikke kan anses at være til hinder for, at en anden end den dataansvarlige myndighed, virksomhed mv. modtager samtykket. Som eksempler fra Datatilsynets praksis kan i den forbindelse peges på, at tilsynet bl.a. har accepteret, at kreditoplysningsbureauer kan udveksle engagementsoplysninger på grundlag af et samtykke givet til den mulige långiver, ligesom tilsynet har accepteret, at der i forbindelse med indhentelse af oplysninger fra SKAT til brug for en vurdering af en låneansøgning kan gives samtykke hertil gennem långiver. Det vil dog altid være den dataansvarlige myndighed, virksomhed mv., som videregiver personoplysningerne, der er ansvarlig for, at der foreligger et gyldigt samtykke hertil, og det kan således ikke fritage den dataansvarlige for ansvar, at der måtte være sket behandling af personoplysninger på grundlag af forkerte eller misvisende oplysninger fra samtykkets modtager, dvs. den myndighed, virksomhed mv., som har modtaget personoplysninger fra den dataansvarlige på baggrund af et ikke-gyldigt samtykke.

Endelig fremgår det om et samtykkes tidsmæssige udstrækning[65], at et sådan ikke er tidsbegrænset, hvorfor det principielt vil kunne anvendes, indtil den registrerede tilbagekalder det, jf. persondatalovens § 38. Det må dog antages, at der vil kunne foreligge sådanne omstændigheder, at et samtykke, der formelt set ikke er tilbagekaldt, ikke bør kunne danne grundlag for behandling af oplysninger. En sådan situation kunne efter omstændighederne foreligge, hvor den dataansvarlige gennem meget lang tid ikke har foretaget behandling af oplysninger om den registrerede. Der henvises i den forbindelse til kravet om god databehandlingsskik i persondatalovens § 5, stk. 1.

2.3.2.9. Begrebet "tredjeland"

Efter persondatalovens § 3, nr. 9, defineres et *tredjeland* som en stat, som ikke indgår i Det Europæiske Fællesskab, og som ikke har gennemført aftaler, der er indgået med Det Europæiske Fællesskab, og som indeholder regler svarende til databeskyttelsesdirektivet.

[63] Persondataloven med kommentarer (2015), s. 174.
[64] Persondataloven med kommentarer (2015), s. 175.
[65] Persondataloven med kommentarer (2015), s. 176 ff.

Af bemærkningerne til persondatalovens § 3, nr. 9, fremgår det, at definitionen af tredjeland har betydning med hensyn til reglerne om lovens geografiske område, jf. § 4, og reglerne om overførsel af oplysninger til tredjelande, jf. § 27.

Det fremgår endvidere af Registerudvalgets betænkning nr. 1345[66], at definitionen *tredjeland* ikke bygger på databeskyttelsesdirektivet. Udvalget foreslog imidlertid definitionen medtaget i persondataloven for at skabe overskuelighed omkring lovens regulering, da begrebet bl.a. vil skulle indarbejdes i lovens § 4 og § 27.

2.3.3. Databeskyttelsesforordningen

Databeskyttelsesforordningens artikel 4 indeholder som nævnt ovenfor 26 definitioner af en række af forordningens centrale begreber. Visse af begreberne er nyskabelser; andre enten svarer til eller er ændrede i forhold til, hvad der følger af databeskyttelsesdirektivet.

2.3.3.1. Begrebet "personoplysninger"

I databeskyttelsesforordningens artikel 4, nr. 1, er begrebet *personoplysninger* nærmere defineret. Omfattet af begrebet personoplysninger er enhver form for information om en identificeret eller identificerbar fysisk person ("den registrerede"); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Ved fastlæggelsen af, hvad der nærmere ligger i begrebet, kan der også lægges vægt på forordningens præambelbetragtning nr. 26, hvoraf det fremgår, at principperne for databeskyttelse bør gælde for enhver information om en identificeret eller identificerbar fysisk person. Det fremgår endvidere af betragtningen, at personoplysninger, der har været genstand for pseudonymisering, og som kan henføres til en fysisk person ved brug af supplerende oplysninger, bør anses for at være oplysninger om en identificerbar fysisk person. Det fremgår endvidere, at for at afgøre om en fysisk person er identificerbar, bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende. Herudover fremgår det af betragtningen, at for at fastslå om midler med rimelighed kan tænkes bragt i anvendelse til at identificere en fysisk person, bør alle objektive forhold tages i betragtning, såsom omkostninger ved og tid der er nødvendig til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling. Det fremgår endvidere af betragtningen, at databeskyttelses-

[66] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 217.

principperne derfor ikke bør gælde for anonyme oplysninger, dvs. oplysninger, der ikke vedrører en identificeret eller identificerbar fysisk person, eller for personoplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres. Endelig fremgår det af betragtningen, at forordningen derfor ikke vedrører behandling af sådanne anonyme oplysninger, herunder til statistiske eller forskningsmæssige formål.

Det fremgår endvidere af præambelbetragtning nr. 30, at fysiske personer kan tilknyttes onlineidentifikatorer, som tilvejebringes af deres enheder, applikationer, værktøjer og protokoller, såsom IP-adresser og cookieidentifikatorer, eller andre identifikatorer, såsom radiofrekvensidentifikationsmærker. Det fremgår desuden af betragtningen, at dette kan efterlade spor, der, navnlig når de kombineres med unikke identifikatorer og andre oplysninger, som serverne modtager, kan bruges til at oprette profiler om fysiske personer og identificere dem.

Herudover fastslås det i præambelbetragtning nr. 27, at forordningen ikke finder anvendelse på personoplysninger om afdøde personer. Det fremgår endvidere af betragtningen, at medlemsstaterne kan fastsætte regler for behandling af personoplysninger om afdøde personer.

2.3.3.2. Begrebet "behandling"
Ifølge databeskyttelsesforordningens artikel 4, nr. 2, skal begrebet *behandling* forstås som enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

2.3.3.3. Begrebet "begrænsning af behandling"
Begrebet *begrænsning af behandling* er i databeskyttelsesforordningens artikel 4, nr. 3, defineret som mærkning af opbevarede personoplysninger med den hensigt at begrænse fremtidig behandling af disse oplysninger.

Af forordningens præambelbetragtning nr. 67 fremgår, at metoder til at begrænse behandlingen af personoplysninger bl.a. kan omfatte, at udvalgte oplysninger midlertidig flyttes til et andet behandlingssystem, at udvalgte personoplysninger gøres utilgængelige for brugere, eller at offentliggjorte oplysninger midlertidig fjernes fra et websted. Det fremgår endvidere af betragtningen, at i automatiske registre bør begrænsning af behandling i princip-

pet sikres ved hjælp af tekniske midler på en sådan måde, at personoplysningerne ikke kan viderebehandles og ikke kan ændres. Endelig fremgår det af betragtningen, at det forhold, at behandling af personoplysninger er begrænset, bør angives tydeligt i systemet.

Definitionen er af betydning for så vidt angår forordningens materielle regler i kapitel III om den registreredes rettigheder, navnlig artikel 18 og 19. Se dog også artikel 58 og artikel 83. Når der i disse bestemmelser i forordningen henvises til begrænsning af behandlingen, vil dette skulle forstås i overensstemmelse med definitionen i artikel 4, nr. 3, af dette begreb.

2.3.3.4. Begrebet "profilering"

Af databeskyttelsesforordningens artikel 4, nr. 4, fremgår det, at ved *profilering* forstås enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser.

Begrebet profilering er nærmere omtalt i forordningens præambelbetragtning nr. 71, hvoraf det fremgår, at den registrerede bør have ret til ikke at blive gjort til genstand for en afgørelse, der kan omfatte en foranstaltning, som evaluerer personlige forhold vedrørende vedkommende, og som alene bygger på automatisk behandling, og som har retsvirkning eller som på tilsvarende vis betydeligt påvirker den pågældende, såsom et automatisk afslag på en onlineansøgning om kredit eller e-rekrutteringsprocedurer uden nogen menneskelig indgriben. Det fremgår endvidere af betragtningen, at en sådan behandling omfatter »profilering«, der består af enhver form for automatisk behandling af personoplysninger, der evaluerer de personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den registreredes arbejdsindsats, økonomisk situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografiske position eller bevægelser, når den har retsvirkning for den pågældende eller på tilsvarende vis betydeligt påvirker den pågældende.

Det fremgår endvidere af betragtning nr. 71, at afgørelser baseret på en sådan behandling, herunder profilering, dog bør være tilladt, når EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt, udtrykkelig tillader det, herunder med henblik på overvågning og forebyggelse af svig og skatteunddragelse i overensstemmelse med EU-institutionernes eller nationale tilsynsmyndigheders forskrifter, standarder og henstillinger og for at garantere sikkerheden og pålideligheden af en tjeneste, der ydes af den dataansvarlige, eller hvis det er nødvendigt for indgåelse eller opfyldelse af en kontrakt mellem

den registrerede og en dataansvarlig, eller når den registrerede har givet sit udtrykkelige samtykke. Det fremgår endvidere af betragtningen, at en sådan behandling under alle omstændigheder bør være omfattet af de fornødne garantier, herunder specifik underretning af den registrerede og retten til menneskelig indgriben, til at fremkomme med synspunkter, til at få en forklaring på den afgørelse, der er truffet efter en sådan evaluering, og til at bestride afgørelsen. Herudover fremgår det, at en sådan foranstaltning ikke bør omfatte et barn.

Det fremgår endvidere af præambelbetragtning nr. 71, at for at sikre en rimelig og gennemsigtig behandling for så vidt angår den registrerede under hensyntagen til de specifikke omstændigheder og forhold, som personoplysningerne behandles under, bør den dataansvarlige anvende passende matematiske eller statistiske procedurer til profileringen, gennemføre tekniske og organisatoriske foranstaltninger, der navnlig kan sikre, at faktorer, der resulterer i unøjagtige personoplysninger, bliver rettet, og at risikoen for fejl minimeres, samt sikre personoplysninger på en måde, der tager højde for de potentielle risici for den registreredes interesser og rettigheder, og som hindrer bl.a. forskelsbehandling af fysiske personer på grund af race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetisk status eller helbredstilstand eller seksuel orientering, eller som resulterer i foranstaltninger, der har en sådan virkning. Endelig fremgår det af præambelbetragtningen, at automatiske afgørelser og profilering baseret på særlige kategorier af personoplysninger kun bør tillades under særlige omstændigheder.

Definitionen er af betydning for så vidt angår forordningens materielle regler i kapitel III om den registreredes rettigheder, navnlig artikel 21 og 22. Se dog også artikel 35, artikel 47 og artikel 70. Når der i disse bestemmelser i forordningen henvises til profilering, vil dette skulle forstås i overensstemmelse med definitionen i artikel 4, nr. 4, af dette begreb.

2.3.3.5. Begrebet "pseudonymisering"

Begrebet *pseudonymisering* er i databeskyttelsesforordningens artikel 4, nr. 5, defineret som behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person.

Definitionen er af betydning for så vidt angår flere af forordningens materielle regler, jf. artikel 6, stik 4, litra e, artikel 25, artikel 32, artikel 40 og artikel 89. Når der i disse bestemmelser i forordningen henvises til pseudonymisering, vil dette skulle forstås i overensstemmelse med definitionen i artikel 4, nr. 5, af dette begreb.

2.3.3.6. Begrebet "register"
Efter databeskyttelsesforordningens artikel 4, nr. 6, forstås ved begrebet *register* enhver struktureret samling af personoplysninger, der er tilgængelig efter bestemte kriterier, hvad enten denne samling er placeret centralt eller decentralt eller er fordelt på funktionsbestemt eller geografisk grundlag.

Herudover fremgår det af forordningens præambelbetragtning nr. 15, at beskyttelsen af fysiske personer bør gælde for både automatisk og manuel behandling af personoplysninger, hvis personoplysningerne er indeholdt eller vil blive indeholdt i et register. Det fremgår endvidere af betragtningen, at sagsmapper eller samlinger af sagsmapper samt deres forsider, som ikke er struktureret efter bestemte kriterier, ikke bør være omfattet af forordningens anvendelsesområde.

2.3.3.7. Begrebet "dataansvarlig"
I databeskyttelsesforordningens artikel 4, nr. 7, defineres begrebet *dataansvarlig* som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret.

2.3.3.8. Begrebet "databehandler"
Ved *databehandler* forstås efter databeskyttelsesforordningens artikel 4, nr. 8, en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.

2.3.3.9. Begrebet "modtager"
Af databeskyttelsesforordningens artikel 4, nr. 9, fremgår det, at begrebet *modtager* defineres som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, hvortil personoplysninger videregives, uanset om det er en tredjemand eller ej. Offentlige myndigheder, som vil kunne få meddelt personoplysninger som led i en isoleret forespørgsel i henhold til EU-retten eller medlemsstaternes nationale ret, anses dog ikke for modtagere.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel III om den registreredes rettigheder. Se dog også artikel 30, artikel 46, artikel 49, artikel 58 samt artikel 83. Når der i disse bestemmelser i forordningen henvises til en modtager, skal dette begreb forstås i overensstemmelse med definitionen i artikel 4, nr. 9.

2.3.3.10. Begrebet "tredjemand"

Begrebet *tredjemand* er i databeskyttelsesforordningens artikel 4, nr. 10, defineret som en anden fysisk eller juridisk person, offentlig myndighed eller institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle personoplysninger.

2.3.3.11. Begrebet "samtykke"

Af databeskyttelsesforordningens artikel 4, nr. 11, fremgår, at ved *samtykke* fra den registrerede forstås enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling.

Det fremgår af forordningens præambelbetragtning nr. 32, at samtykke bør gives i form af en klar bekræftelse, der indebærer en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved vedkommende accepterer, at personoplysninger om vedkommende behandles, f.eks. ved en skriftlig erklæring, herunder elektronisk, eller en mundtlig erklæring. Det fremgår endvidere af betragtningen, at dette f.eks. kan foregå ved at sætte kryds i et felt ved besøg på et websted, ved valg af tekniske indstillinger til informationssamfundstjenester eller en anden erklæring eller handling, der tydeligt i denne forbindelse tilkendegiver den registreredes accept af den foreslåede behandling af vedkommendes personoplysninger. Herudover fremgår det af betragtningen, at tavshed, forudafkrydsede felter eller inaktivitet derfor ikke bør udgøre samtykke. Desuden fremgår det, at samtykke bør dække alle behandlingsaktiviteter, der udføres til det eller de samme formål. Det fremgår endvidere, at når behandling tjener flere formål, bør der gives samtykke til dem alle. Endelig fremgår det af præambelbetragtningen, at hvis den registreredes samtykke skal gives efter en elektronisk anmodning, skal anmodningen være klar, kortfattet og ikke unødigt forstyrre brugen af den tjeneste, som samtykke gives til.

Endvidere fremgår det af præambelbetragtning nr. 42 i forordningen, at hvis behandling er baseret på den registreredes samtykke, bør den dataansvarlige kunne påvise, at den registrerede har givet samtykke til behandlingen. Herudover fremgår det, at navnlig i forbindelse med skriftlige erklæringer om andre forhold bør garantier sikre, at den registrerede er bekendt med, at og i hvilket omfang der er givet samtykke. Det fremgår endvidere, at – i overensstemmelse med Rådets direktiv 93/13/EØF – bør der stilles en samtykkeerklæring udformet af den dataansvarlige til rådighed i en letforståelig og lettilgængelig form og i et klart og enkelt sprog, og den bør ikke indeholde urimelige vilkår. Det fremgår desuden, at for at sikre, at samtykket er informeret, bør den registrerede som minimum være bekendt med den dataansvarliges identitet og formålene med den behandling, som personoplysnin-

gerne skal bruges til. Endelig fremgår det af betragtningen, at samtykke ikke bør anses for at være givet frivilligt, hvis den registrerede ikke har et reelt eller frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende.

Det fremgår endelig også af forordningens præambelbetragtning nr. 43, at med henblik på at sikre, at der frivilligt er givet samtykke, bør samtykke ikke udgøre et gyldigt retsgrundlag for behandling af personoplysninger i et specifikt tilfælde, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige, navnlig hvis den dataansvarlige er en offentlig myndighed, og det derfor er usandsynligt, at samtykket er givet frivilligt under hensyntagen til alle de omstændigheder, der kendetegner den specifikke situation. Det fremgår endvidere af betragtningen, at samtykke formodes ikke at være givet frivilligt, hvis det ikke er muligt at give særskilt samtykke til forskellige behandlingsaktiviteter vedrørende personoplysninger, selv om det er hensigtsmæssigt i det enkelte tilfælde, eller hvis opfyldelsen af en kontrakt, herunder ydelsen af en tjeneste, gøres afhængig af samtykke, selv om et sådant samtykke ikke er nødvendigt for dennes opfyldelse.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel II om principper, navnlig artikel 6-9. Se dog også artikel 13-14, artikel 17-18, artikel 20, artikel 22, artikel 40, artikel 49 og artikel 83. Når der i disse bestemmelser i forordningen henvises til samtykke, skal dette begreb forstås i overensstemmelse med definitionen i artikel 4, nr. 11.

2.3.3.12. Begrebet "brud på persondatasikkerheden"

I databeskyttelsesforordningens artikel 4, nr. 12, defineres, hvad der skal forstås ved *brud på persondatasikkerheden*. Efter denne bestemmelse skal dette begreb således forstås som brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Definitionen er navnlig af betydning for så vidt angår forordningens artikel 33 og artikel 34. Se dog også artikel 49, artikel 58 og artikel 70. Når der i disse bestemmelser i forordningen henvises til brud på persondatasikkerheden, skal dette begreb forstås i overensstemmelse med definitionen i artikel 4, nr. 12.

2.3.3.13. Begrebet "genetiske data"

I medfør af databeskyttelsesforordningens artikel 4, nr. 13, skal ved *genetiske data* forstås personoplysninger vedrørende en fysisk persons arvede eller erhvervede genetiske karakteristika, som giver entydig information om den fysiske persons fysiologi eller helbred, og

som navnlig foreligger efter en analyse af en biologisk prøve fra den pågældende fysiske person.

Det fremgår endvidere af forordningens præambelbetragtning nr. 34, at genetiske data bør defineres som personoplysninger vedrørende en fysisk persons arvede eller erhvervede genetiske karakteristika, som foreligger efter en analyse af en biologisk prøve fra den pågældende fysiske person, navnlig en analyse på kromosomniveau, af deoxyribonukleinsyre (DNA) eller af ribonukleinsyre (RNA), eller efter en analyse af et andet element til indhentning af lignende oplysninger.

2.3.3.14. Begrebet "biometriske data"

Efter databeskyttelsesforordningens artikel 4, nr. 14, betyder *biometriske data* personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger.

Af forordningens præambelbetragtning nr. 51 fremgår bl.a., at behandling af fotografier ikke systematisk bør anses for at være behandling af særlige kategorier af personoplysninger, eftersom de kun vil være omfattet af definitionen af biometriske data, når de behandles ved en specifik teknisk fremgangsmåde, der muliggør entydig identifikation eller autentifikation af en fysisk person.

2.3.3.15. Begrebet "helbredsoplysninger"

Ved *helbredsoplysninger* skal efter databeskyttelsesforordningens artikel 4, nr. 15, forstås personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand.

Ved fastlæggelsen af, hvad der nærmere skal forstås ved begrebet, kan der også lægges vægt på databeskyttelsesforordningens præambelbetragtning nr. 35, hvoraf det fremgår, at helbredsoplysninger bør omfatte alle personoplysninger om den registreredes helbredstilstand, som giver oplysninger om den registreredes tidligere, nuværende eller fremtidige fysiske eller mentale helbredstilstand. Det fremgår endvidere af betragtningen, at dette omfatter oplysninger om den fysiske person indsamlet i løbet af registreringen af denne med henblik på eller under levering af sundhedsydelser, jf. Europa-Parlamentets og Rådets direktiv 2011/24/EU, til den fysiske person; et nummer, symbol eller særligt mærke, der tildeles en fysisk person for entydigt at identificere den fysiske person til sundhedsformål; oplysninger, der hidrører fra prøver eller undersøgelser af en legemsdel eller legemlig substans, herunder fra genetiske data og biologiske prøver; og enhver oplysning om f.eks. en

sygdom, et handicap, en sygdomsrisiko, en sygehistorie, en sundhedsfaglig behandling eller den registreredes fysiologiske eller biomedicinske tilstand uafhængigt af kilden hertil, f.eks. fra en læge eller anden sundhedsperson, et hospital, medicinsk udstyr eller in vitro-diagnostik.

2.3.3.16. Begrebet "hovedvirksomhed"

Det følger af databeskyttelsesforordningens artikel 4, nr. 16, at *hovedvirksomhed* skal forstås som: a) for så vidt angår en dataansvarlig, som er etableret i mere end én medlemsstat, stedet for dennes centrale administration i Unionen, medmindre beslutninger vedrørende formål og hjælpemidler i forbindelse med behandling af personoplysninger træffes i en anden af den dataansvarliges etableringer i Unionen, og sidstnævnte etablering har beføjelse til få sådanne beslutninger gennemført; i så fald anses den etablering, der har truffet sådanne beslutninger, for hovedvirksomheden, b) for så vidt angår en databehandler, som er etableret i mere end én medlemsstat, stedet for dennes centrale administration i Unionen, eller, hvis denne ikke har en central administration i Unionen, den etablering i Unionen, hvor databehandlerens hovedbehandlingsaktiviteter foretages i databehandlerens egenskab af at være databehandler, i det omfang databehandleren er underlagt specifikke forpligtelser i henhold til denne forordning.

Om begrebet hovedvirksomhed fremgår endvidere af præambelbetragtning nr. 36, at den dataansvarliges hovedvirksomhed i Unionen bør være stedet for dennes centrale administration i Unionen, medmindre der træffes beslutninger vedrørende formål og hjælpemidler i forbindelse med behandling af personoplysninger et andet sted i Unionen, hvor den dataansvarlige er etableret; i dette tilfælde bør dette andet sted anses for at være hovedvirksomheden. Det fremgår endvidere af betragtningen, at en dataansvarligs hovedvirksomhed i Unionen bør fastlægges ud fra objektive kriterier og bør indebære effektiv og faktisk udøvelse af ledelsesaktiviteter, der fastlægger de vigtigste beslutninger om behandlingsformål og -hjælpemidler gennem en mere permanent struktur. Herudover fremgår det, at dette kriterium ikke bør afhænge af, om behandling af personoplysninger foretages på dette sted. Endvidere fremgår det af betragtningen, at det forhold, at der findes og anvendes tekniske midler og teknologi til behandling af personoplysninger eller behandlingsaktiviteter, ikke i sig selv medfører, at der er etableret en hovedvirksomhed, og derfor ikke er afgørende for kriteriet om hovedvirksomhed.

Herudover fremgår det af præambelbetragtning nr. 36, at databehandlerens hovedvirksomhed bør være stedet for den pågældendes centrale administration i Unionen, eller hvis databehandleren ikke har nogen central administration i Unionen, det sted, hvor hovedbehandlingsaktiviteterne foregår i Unionen. Det fremgår endvidere, at i tilfælde, der involverer både den dataansvarlige og databehandleren, bør den kompetente ledende tilsynsmyndig-

hed fortsat være tilsynsmyndigheden i den medlemsstat, hvor den dataansvarlige har sin hovedvirksomhed, men databehandlerens tilsynsmyndighed bør anses for at være en berørt tilsynsmyndighed, og denne tilsynsmyndighed bør deltage i den samarbejdsprocedure, der er fastsat i forordningen. Herudover fremgår det, at under alle omstændigheder bør tilsynsmyndighederne i den eller de medlemsstater, hvor databehandleren har en eller flere etableringer, ikke anses for at være berørte tilsynsmyndigheder, når et udkast til afgørelse kun vedrører den dataansvarlige. Endelig fremgår det af betragtningen, at hvis behandlingen foretages af en koncern, bør den kontrollerende virksomheds hovedvirksomhed anses for at være koncernens hovedvirksomhed, medmindre formål og hjælpemidler fastlægges af en anden virksomhed.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel VI om uafhængige tilsynsmyndigheder, navnlig artikel 56 om den ledende tilsynsmyndigheds kompetence. Det fremgår således af denne bestemmelses stk. 1, at uden, at det berører artikel 55, er tilsynsmyndigheden for den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering kompetent til at fungere som ledende tilsynsmyndighed for den grænseoverskridende behandling, der foretages af denne dataansvarlige eller databehandler efter proceduren i artikel 60. Se foruden artikel 60 dog også artikel 65 i forordningens kapitel VII om samarbejde og sammenhæng. Når der i disse bestemmelser i forordningen henvises til hovedvirksomhed, skal dette begreb forstås i overensstemmelse med definitionen i artikel 4, nr. 16.

2.3.3.17. Begrebet "repræsentant"

Begrebet *repræsentant* skal efter databeskyttelsesforordningens artikel 4, nr. 17, forstås som en fysisk eller juridisk person, der er etableret i Unionen, som skriftligt er udpeget af den dataansvarlige eller databehandleren i henhold til artikel 27, og som repræsenterer den dataansvarlige eller databehandleren hvad angår deres respektive forpligtelser i medfør af denne forordning.

Om udpegning af en repræsentant fremgår det af præambelbetragtning nr. 80 i forordningen, at hvis en dataansvarlig eller en databehandler, som ikke er etableret i Unionen, behandler personoplysninger om registrerede, der er i Unionen, og hvis behandlingsaktiviteter vedrører udbud af varer eller tjenesteydelser til sådanne registrerede i Unionen, uanset om betaling fra de registrerede er påkrævet, eller overvågning af deres adfærd, hvis adfærden finder sted i Unionen, bør den dataansvarlige eller databehandleren udpege en repræsentant, medmindre behandlingen er lejlighedsvis, ikke i stort omfang indebærer behandling af særlige kategorier af personoplysninger eller behandlingen af personoplysninger vedrørende straffedomme og lovovertrædelser, og sandsynligvis ikke indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder under hensyntagen til behandlingens

karakter, sammenhæng, omfang og formål, eller hvis den dataansvarlige er en offentlig myndighed eller et offentligt organ.

Det fremgår endvidere af betragtning nr. 80, at repræsentanten bør handle på den dataansvarliges eller databehandlerens vegne og kan kontaktes af enhver tilsynsmyndighed. Herudover fremgår det, at repræsentanten udtrykkelig bør udpeges ved et skriftligt mandat fra den dataansvarlige eller fra databehandleren til at handle på dennes vegne for så vidt angår dennes forpligtelser i henhold til denne forordning. Endvidere fremgår det af betragtningen, at udpegelsen af en sådan repræsentant ikke berører den dataansvarliges eller databehandlerens ansvar, herunder erstatningsansvar, i henhold til denne forordning. Det fremgår desuden, at en sådan repræsentant bør udføre sine opgaver i overensstemmelse med mandatet fra den dataansvarlige eller databehandleren, herunder samarbejde med de kompetente tilsynsmyndigheder med hensyn til enhver foranstaltning, der træffes for at sikre overholdelse af denne forordning. Endelig fremgår det af betragtningen, at den udpegede repræsentant bør være underlagt håndhævelsesforanstaltninger i tilfælde af manglende overholdelse fra den dataansvarliges eller databehandlerens side.

Definitionen er ikke kun af betydning for så vidt angår forordningens artikel 27. Begrebet repræsentant indgår således også i forordningens artikel 13-14, artikel 30-31, artikel 35 og artikel 58. Når der i disse bestemmelser henvises til en repræsentant, skal dette forstås i overensstemmelse med forordningens definition i artikel 4, nr. 17.

2.3.3.18. Begrebet "foretagende"

Efter databeskyttelsesforordningens artikel 4, nr. 18, forstås ved begrebet *foretagende* en fysisk eller juridisk person, som udøver økonomisk aktivitet, uanset dens retlige status, herunder partnerskaber eller sammenslutninger, der regelmæssigt udøver økonomisk aktivitet.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel V om overførsler af personoplysninger til tredjelande eller internationale organisationer. Se dog også artikel 30 og artikel 88. Når der i disse bestemmelser henvises til et foretagende eller en gruppe af foretagender, skal dette forstås i overensstemmelse med forordningens definition i artikel 4, nr. 18.

2.3.3.19. Begrebet "koncern"

Ved *koncern* skal efter databeskyttelsesforordningens artikel 4, nr. 19, forstås en virksomhed, der udøver kontrol, og de af denne kontrollerede virksomheder.

Om begrebet koncern fremgår det af præambelbetragtning nr. 37 i forordningen, at en koncern bør omfatte en virksomhed, der udøver kontrol, og de af denne kontrollerede virksomheder, hvor den kontrollerende virksomhed bør være den virksomhed, der kan udøve bestemmende indflydelse på de øvrige virksomheder, f.eks. i kraft af ejendomsret, finansiel deltagelse eller de regler, den er underlagt, eller beføjelsen til at få gennemført regler om beskyttelse af personoplysninger. Det fremgår endvidere af betragtningen, at en virksomhed, der udøver kontrol med behandlingen af personoplysninger i de virksomheder, der er knyttet til den, sammen med disse virksomheder bør anses som en koncern.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel V om overførsler af personoplysninger til tredjelande eller internationale organisationer. Se dog også artikel 36-37 og artikel 88. Når der i disse bestemmelser henvises til en koncern, skal dette forstås i overensstemmelse med forordningens definition i artikel 4, nr. 19.

2.3.3.20. Begrebet "bindende virksomhedsregler"

Af artikel 4, nr. 20, i databeskyttelsesforordningen fremgår det, at *bindende virksomhedsregler* skal forstås som regler om beskyttelse af personoplysninger, som en dataansvarlig eller databehandler, der er etableret på en medlemsstats område, overholder i forbindelse med overførsel eller en række overførsler af personoplysninger til en dataansvarlig eller databehandler i et eller flere tredjelande inden for en koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet.

Med hensyn til hvornår bindende virksomhedsregler kan benyttes, fremgår det af forordningens præambelbetragtning nr. 110, at en koncern eller en gruppe af foretagender, der udøver en fælles økonomisk aktivitet, bør kunne benytte godkendte bindende virksomhedsregler for sine internationale overførsler fra Unionen til organisationer inden for samme koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet, forudsat at sådanne virksomhedsregler omfatter alle væsentlige principper og rettigheder, som kan håndhæves, med henblik på at sikre de fornødne garantier for overførsel eller kategorier af overførsler af personoplysninger.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel V om overførsel af personoplysninger til tredjelande, navnlig artikel 47. Når der i denne artikel og i forordningen i øvrigt henvises til bindende virksomhedsregler, skal dette begreb forstås i overensstemmelse med forordningens definition i artikel 4, nr. 20.

2.3.3.21. Begrebet "tilsynsmyndighed"
Begrebet *tilsynsmyndighed* er i databeskyttelsesforordningens artikel 4, nr. 21, defineret som en uafhængig offentlig myndighed, der er etableret i en medlemsstat i henhold til artikel 51.

I forordningens præambelbetragtning nr. 117 fremgår om oprettelse af en tilsynsmyndighed, at oprettelse af tilsynsmyndigheder i medlemsstaterne, som har beføjelser til at udføre deres opgaver og udøve deres beføjelser i fuld uafhængighed, har afgørende betydning for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger. Det fremgår endvidere af betragtningen, at medlemsstaterne bør kunne oprette mere end én tilsynsmyndighed for at afspejle deres forfatningsmæssige, organisatoriske og administrative struktur.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel VI om uafhængige tilsynsmyndigheder og kapitel VII om samarbejde og sammenhæng. Når der i bestemmelser i disse to kapitler henvises til en eller flere tilsynsmyndigheder, skal dette begreb forstås i overensstemmelse med forordningens definition i artikel 4, nr. 21.

2.3.3.22. Begrebet "berørt tilsynsmyndighed"
Efter databeskyttelsesforordningens artikel 4, nr. 22, forstås ved *berørt tilsynsmyndighed* en tilsynsmyndighed, der er berørt af en behandling af personoplysninger, fordi: *a)* den dataansvarlige eller databehandleren er etableret på denne tilsynsmyndigheds medlemsstats område, *b)* de registrerede, der har bopæl i denne tilsynsmyndigheds medlemsstat, i væsentlig grad er påvirket af eller sandsynligvis i væsentlig grad vil kunne blive påvirket af behandlingen, eller *c)* en klage er blevet indgivet til denne tilsynsmyndighed.

Ved fastlæggelsen af, hvad der nærmere skal forstås ved begrebet, kan der også lægges vægt på databeskyttelsesforordningens præambelbetragtning nr. 36, 6. og 7. punktum, hvoraf det fremgår, at i tilfælde, der involverer både den dataansvarlige og databehandleren, bør den kompetente ledende tilsynsmyndighed fortsat være tilsynsmyndigheden i den medlemsstat, hvor den dataansvarlige har sin hovedvirksomhed, men databehandlerens tilsynsmyndighed bør anses for at være en berørt tilsynsmyndighed, og denne tilsynsmyndighed bør deltage i den samarbejdsprocedure, der er fastsat i denne forordning. Under alle omstændigheder bør tilsynsmyndighederne i den eller de medlemsstater, hvor databehandleren har en eller flere etableringer, ikke anses for at være berørte tilsynsmyndigheder, når et udkast til afgørelse kun vedrører den dataansvarlige.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel VII om samarbejde og sammenhæng. Når der i disse bestemmelser henvises til den eller de berørte tilsynsmyndighed(er), skal dette begreb forstås i overensstemmelse med forordningens definition i artikel 4, nr. 22.

2.3.3.23. Begrebet "grænseoverskridende behandling"

Ved *grænseoverskridende behandling* forstås efter databeskyttelsesforordningens artikel 4, nr. 23: *a)* behandling af personoplysninger, der finder sted som led i aktiviteter, som udføres for en dataansvarligs eller en databehandlers virksomheder i mere end én medlemsstat i Unionen, hvor den dataansvarlige eller databehandleren er etableret i mere end én medlemsstat, eller *b)* behandling af personoplysninger, der finder sted som led i aktiviteter, som udføres for en dataansvarligs eller en databehandlers eneste etablering i Unionen, men som i væsentlig grad påvirker eller sandsynligvis i væsentlig grad vil kunne påvirke registrerede i mere end én medlemsstat.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel VI om uafhængige tilsynsmyndigheder, navnlig artikel 56 om den ledende tilsynsmyndigheds kompetence. Det fremgår således af denne bestemmelses stk. 1, at uden, at det berører artikel 55, er tilsynsmyndigheden for den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering kompetent til at fungere som ledende tilsynsmyndighed for den grænseoverskridende behandling, der foretages af denne dataansvarlige eller databehandler efter proceduren i artikel 60. Når der i denne bestemmelse i forordningen henvises til grænseoverskridende behandling, skal dette begreb forstås i overensstemmelse med definitionen i artikel 4, nr. 23.

2.3.3.24. Begrebet "relevant og begrundet indsigelse"

Ifølge databeskyttelsesforordningens artikel 4, nr. 24, forstås ved *relevant og begrundet indsigelse* en indsigelse mod et udkast til afgørelse om, hvorvidt der foreligger en overtrædelse af denne forordning, eller hvorvidt en planlagt foranstaltning i forbindelse med den dataansvarlige eller databehandleren overholder denne forordning, og som klart påviser betydningen af de risici, som udkastet til afgørelse udgør for registreredes grundlæggende rettigheder og frihedsrettigheder og, hvis det er relevant, for den frie udveksling af personoplysninger i Unionen.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel VII om samarbejde og sammenhæng, navnlig artikel 60 om samarbejde mellem den ledende tilsynsmyndighed og de andre berørte tilsynsmyndigheder. Det fremgår således af stk. 4 i denne bestemmelse, at hvis en af de andre berørte tilsynsmyndigheder inden for fire uger efter at være blevet hørt, jf. artikel 60, stk. 3, fremkommer med en relevant og be-

grundet indsigelse mod udkastet til afgørelse, forelægger den ledende tilsynsmyndighed, hvis den ikke følger den relevante og begrundede indsigelse eller er af den opfattelse, at indsigelsen ikke er relevant eller begrundet, sagen for den sammenhængsmekanisme, der er omhandlet i artikel 63. Når der i disse bestemmelser henvises til en relevant og begrundet indsigelse, skal dette begreb forstås i overensstemmelse med forordningens definition i artikel 4, nr. 24.

Det er i den forbindelse også værd at notere sig, at det fremgår af forordningens præambel betragtning nr. 124, sidste punktum, at Databeskyttelsesrådet inden for rammerne af sine opgaver med at udstede retningslinjer om ethvert spørgsmål vedrørende anvendelsen af denne forordning navnlig bør kunne udstede retningslinjer om, hvilke kriterier der skal tages i betragtning for at fastlægge, hvorvidt en behandling i væsentlig grad påvirker registrerede i mere end én medlemsstat, og hvad der udgør en relevant og begrundet indsigelse.

2.3.3.25. Begrebet informationssamfundstjeneste

Af databeskyttelsesforordningens artikel 4, nr. 25, fremgår det, at *informationssamfundstjeneste* skal forstås som en tjeneste som defineret i artikel 1, stk. 1, litra b, i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535.

Direktivet, der henvises til, er Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationstjenester.[67] Af dette direktivs artikel 1, stk. 1, litra b, fremgår, at der ved begrebet "tjeneste" forstås enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager.

Det fremgår i øvrigt af direktivet, at det er udtryk for en kodificering af informationsproceduredirektivet fra 1998[68], som er gennemført i dansk ret ved Erhvervsministeriets bekendtgørelse nr. 190 af 20. marts 2001 om EU's informationsprocedure for tekniske standarder og forskrifter samt forskrifter for informationssamfundets tjenester, der nu er ændret til bekendtgørelse nr. 1087 af 8. juli 2016.

Den definition på begrebet informationssamfundstjeneste, som er indeholdt i forordningens artikel 4, nr. 25 er navnlig af betydning, for så vidt angår forordningens materielle regel om

67 Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).

68 Europa-Parlamentets og Rådets direktiv 98/34/EF om en informationsprocedure med hensyn til tekniske standarder og forskrifter samt forskrifter for informationssamfundets tjenester (EFT 1998 L 204 s. 37) med senere ændringer.

betingelser for et barns samtykke i forbindelse med informationssamfundstjenester. Se dog også artikel 17 og artikel 21. Når der i disse bestemmelser i forordningen henvises til en informationssamfundstjeneste eller informationssamfundstjenester, skal dette begreb forstås i overensstemmelse med definition i artikel 4, nr. 25.

Det bemærkes, at informationssamfundstjenester direkte til børn efter artikel 8, stk. 1, må antages eksempelvis at kunne omfatte Facebook, Instagram og Snapchat. Der henvises i øvrigt til afsnit 3.6. om børns samtykke i forbindelse med informationssamfundstjenester, artikel 8.

2.3.3.26. Begrebet "international organisation"
Det fremgår af databeskyttelsesforordningens artikel 4, nr. 26, at der ved begrebet *international organisation* forstås en folkeretlig organisation og organer, der er underordnet den, samt ethvert andet organ, der er oprettet ved eller med hjemmel i en aftale mellem to eller flere lande.

Definitionen er navnlig af betydning for så vidt angår forordningens materielle regler i kapitel V om overførsler af personoplysninger til tredjelande og internationale organisationer. Se dog også artikel 13-15, artikel 30, artikel 40 og 42, artikel 50 samt artikel 70-71. Når der i disse bestemmelser i forordningen henvises til en international organisation eller internationale organisationer, skal dette begreb forstås i overensstemmelse med definitionen i artikel 4, nr. 26.

2.3.4. Overvejelser
Databeskyttelsesforordningens artikel 4 indeholder definitioner, som i vidt omfang svarer til definitionerne i artikel 2 i databeskyttelsesdirektivet, jf. således definitionerne af de helt centrale begreber som personoplysninger, behandling, register, dataansvarlig, databehandler, modtager og tredjemand. Det må derfor antages, at det er muligt at videreføre den gældende retstilstand – og Datatilsynets praksis vedrørende disse begreber – når forordningen får virkning 25. maj 2018. For så vidt angår definitionen af samtykke henvises der til konklusionen i afsnit om samtykke.

Når der i databeskyttelsesforordningens artikel 4, nr. 2, tales om "automatisk behandling" må dette i øvrigt antages at svare til begrebet "elektronisk databehandling", som er nævnt i persondatalovens § 3, nr. 2, og databeskyttelsesdirektivets artikel 2, litra b.

Særligt for så vidt angår oplysninger om *afdøde* personer bemærkes, at som nævnt ovenfor under pkt. 2.3.3.1. finder databeskyttelsesforordningen ikke anvendelse på personoplys-

ninger om afdøde personer, men de enkelte medlemsstater kan vælge at fastsætte regler for behandling af personoplysninger om afdøde personer, jf. præambelbetragtning nr. 27.

Det er således muligt at fastsætte regler om, at Datatilsynets hidtidige praksis om afdøde personer skal videreføres, når forordningen får virkning fra den 25. maj 2018. Vælger man fra dansk side ikke at fastsætte sådanne særlige regler, vil oplysninger om afdøde personer ikke være omfattet af databeskyttelsesforordningen.

Af punkt 2.3.2.1. ovenfor fremgår det endvidere bl.a., at oplysninger om *fostre* – ligesom efter den hidtidige registerlovgivning – i almindelighed vil falde ind under begrebet personoplysninger, og at det må være op til Datatilsynet i praksis at fastsætte, hvad dette indebærer i forhold til bl.a. persondatalovens bestemmelser om samtykke og den registreredes rettigheder.

I modsætning til oplysninger om afdøde personer er databeskyttelsesforordningen tavs i forhold til, om, og i givet fald i hvilket omfang, oplysninger om fostre kan antages at være en personoplysning i forordningens artikel 4, nr. 1's forstand. Det må derfor afklares i praksis, hvorvidt oplysninger om fostre vil kunne antages for værende omfattet af databeskyttelsesforordningens artikel 4, nr. 1's definition af personoplysninger.

For så vidt angår det danske registerbegreb henvises til særskilt afsnit herom.

Dog bemærkes, at der ovenfor er redegjort for det nye begreb *begrænsning i behandling*. Begrebet minder om det begreb, der i databeskyttelsesdirektivet og persondataloven omtales som *blokering*, jf. herved f.eks. databeskyttelsesdirektivets artikel 2, litra b, og persondatalovens § 37. Der vurderes derfor umiddelbart at være overensstemmelse mellem begrebet *begrænsning i behandling* og *blokering*, hvorfor eventuel tidligere praksis vedrørende blokering må antages at kunne videreføres.

2.4. Det danske registerbegreb

2.4.1. Præsentation

Af Registerudvalgets betænkning nr. 1345 fremgår[69], at udvalget ifølge dets kommissorium bl.a. havde fået til opgave at overveje og vurdere, hvorledes en fremtidig lovgivning om behandling af personoplysninger mv. bør udformes, således at der opnås den rette balance mellem på den ene side hensynet til at sikre borgernes privatliv og personlige integritet og på den anden side hensynet til at bevare og til stadighed udbygge en effektiv offent-

[69] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 13 ff.

lig administration og et privat erhvervsliv, som ikke pålægges unødige byrder. Udvalget skulle i den forbindelse bl.a. overveje, om en sådan lovgivning skal omfatte alle former for behandling af personoplysninger, uanset om behandlingen foretages manuelt eller ved hjælp af edb.

Når sidstnævnte blev gjort til et særligt tema under Registerudvalgets arbejde, skyldes det, at databeskyttelsesdirektivet i artikel 2, litra c, indeholdt en definition af begrebet register. Den dagældende registerlovgivning indeholdt derimod kun en definition af begrebet edb-registre.[70] En legal definition på et manuelt register var således ikke medtaget i lovgivningen. Ved afgørelsen af hvilke manuelle oplysninger, som var omfattet af lov om private registre, ville man derfor nærmere skulle undersøge bemærkningerne til bestemmelsen i lovens § 1, stk. 1.

Databeskyttelsesforordningen indeholder i artikel 4, nr. 6, en definition af begrebet "register", der svarer til definitionen i direktivet. Spørgsmålet er herefter, hvorvidt det er muligt at videreføre den danske fortolkning af databeskyttelsesdirektivets definition af registergrebet, som der er redegjort for nærmere i Registerudvalgets betænkning, når forordningen får virkning 25. maj 2018.

2.4.2. Gældende ret

2.4.2.1. Persondatalovens registerbegreb og baggrunden herfor

Det fremgår af persondatalovens § 3, nr. 3, at et *register* er enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grundlag.

Begrebet register skal ses i sammenhæng med, at det af persondatalovens § 1, stk. 1, bl.a. fremgår, at loven gælder for behandling af personoplysninger, der er eller vil blive indeholdt i et register. Afgrænsningen af registerbegrebet har således betydning for, om en behandling er omfattet af loven eller ej.

Af bemærkningerne til persondatalovens § 3, nr. 3[71], fremgår det, at bestemmelsens registerbegreb omfatter manuelle registre, såsom fortegnelser, kartotekskasser, journalsystemer og andre samlinger af manuelt materiale, som er opbevaret struktureret efter bestemte kriterier vedrørende personer for at lette adgangen til de indeholdte personoplysninger. Derimod er manuelle akter, som indgår i den dataansvarliges konkrete sagsbehandling, mapper

[70] § 1, stk. 2, i bekendtgørelse af lov om offentlige myndigheders registre, jf. lovbekendtgørelse nr. 654 af 20. september 1991.
[71] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.

med sagsakter eller samlinger af sådanne mapper, ikke omfattet af registerbegrebet. Endelig fremgår det, at den nærmere afgrænsning af registerbegrebet må finde sted gennem Datatilsynets praksis.

Persondatalovens § 3, nr. 3, bygger på databeskyttelsesdirektivets artikel 2, litra c. Efter denne bestemmelse skal der ved begrebet register forstås enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grundlag.

Det fremgår endvidere af direktivets præambelbetragtning nr. 15, at behandling af sådanne oplysninger kun er omfattet af direktivet, hvis den foregår ved hjælp af elektronisk databehandling, eller hvis de pågældende oplysninger er indeholdt i eller skal indgå i et register, der er struktureret efter bestemte kriterier vedrørende personerne for at lette adgangen til de pågældende personoplysninger.

For så vidt angår manuel behandling, fremgår det af direktivets præambelbetragtning nr. 27, at direktivet kun omfatter registre og ikke sagsmapper, der ikke er strukturerede; navnlig skal indholdet af et register være struktureret efter bestemte kriterier vedrørende personer for at lette adgangen til personoplysningerne; i overensstemmelse med definitionen i artikel 2, litra c), kan de forskellige kriterier, der gør det muligt at bestemme de enkelte dele i en struktureret samling af personoplysninger, samt de forskellige kriterier for adgang til denne samling af oplysninger defineres af hver enkelt medlemsstat; sagsmapper eller samlinger af sagsmapper eller deres forsider, som ikke er struktureret efter bestemte kriterier, hører under ingen omstændigheder ind under dette direktivs anvendelsesområde.

Af Registerudvalgets betænkning nr. 1345[72] fremgår bl.a., at der i den gældende registerlovgivning er indeholdt en definition på begrebet edb-registre, jf. lov om offentlige myndigheders registre § 1, stk. 2. Registerudvalget anførte endvidere, at en legal definition på et manuelt register derimod ikke er medtaget i lovgivningen. Ved afgørelsen af hvilke manuelle oplysninger, som er omfattet af lov om private registre, vil man derfor, ifølge Registerudvalget, nærmere skulle undersøge bemærkningerne til bestemmelsen i lovens § 1, stk. 1.

Registerudvalget anførte endvidere, at direktivets artikel 2, litra c, i modsætning hertil, indeholder en definition på begrebet "register". Efter denne bestemmelse skal der ved begrebet "register", ifølge Registerudvalget, forstås enhver struktureret samling af personop-

[72] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 213 ff.

lysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grundlag.

Det fremgår endvidere af Registerudvalgets betænkning nr. 1345, at bestemmelsen, som er af central betydning ved fastlæggelsen af direktivets funktionelle anvendelsesområde, jf. artikel 3, stk. 1, bl.a. på dansk initiativ blev undergivet indgående drøftelser i forbindelse med vedtagelsen af direktivet. Fra dansk side blev der, ifølge Registerudvalget, lagt afgørende vægt på, at et direktiv på området ikke måtte komme til også at omfatte personoplysninger, som indgår i konkrete manuelle sagsakter/mapper eller samlinger heraf i den offentlige forvaltning. Til støtte herfor anførtes en række grunde, herunder bl.a. at personoplysninger, der behandles under de nævnte former, i dag er reguleret i dansk ret på en måde, der tilsikrer de pågældende personers integritet. Oplysninger, der ikke indgår i et edb-register i den offentlige sektor, var således, ifølge Registerudvalget, omfattet af reglerne i en generel lov vedrørende sagsbehandling (forvaltningsloven) samt af reglerne i en generel lov vedrørende offentlighedens adgang til dokumenter i den offentlige forvaltning (offentlighedsloven). Med hensyn til oplysninger, der indgår i manuelle sager, der er afsluttet, overgår disse - efter en vis årrække - til at være omfattet af lov om offentlige arkiver, der bl.a. indeholder regler vedrørende tilgængelighed mv.

Det fremgår endvidere af Registerudvalgets betænkning nr. 1345, at der under forhandlingerne viste sig ikke at være flertal for helt at holde manuelle personoplysninger uden for direktivets område. Direktivet kom derfor i dets endelige form til også at omfatte manuelle personoplysninger, som er eller vil blive indeholdt i et register.

Herudover fremgår det af betænkningen, at betragtning nr. 15 og 17 blev indsat i præamblen til belysning af, hvornår der er tale om et register i direktivets forstand. Endvidere blev der til Rådets mødeprotokol afgivet en erklæring (nr. 7), hvoraf det bl.a. fremgår, at de kriterier, som danner baggrund for fastlæggelse af de elementer, som tilsammen udgør en struktureret samling af personoplysninger, samt de kriterier, hvorefter en sådan samling er tilgængelig, skal præciseres af hver enkelt medlemsstat, samt at sager og samlinger af sager, inkl. titelblad, ikke er omfattet af definitionen, hvis deres indhold ikke har karakter af et register.

De nævnte betragtninger, herunder navnlig betragtning 27, sammenholdt med den nævnte erklæring til Rådets mødeprotokol, var, ifølge Registerudvalget, en imødekommelse af de danske ønsker med hensyn til spørgsmålet om manuelle oplysninger i den offentlige forvaltning. Dette gælder særligt med hensyn til bemærkningen om, at sagsmapper eller samlinger af sagsmapper eller deres forsider, som ikke er struktureret efter bestemte kriterier, under ingen omstændigheder hører ind under direktivets anvendelsesområde. Det fremgår

endvidere af betænkningen, at tilsvarende gælder med hensyn til bemærkningen i mødeprotokolerklæringen om, at det er overladt til medlemsstaterne selv nærmere at præcisere indholdet af det manuelle registerbegreb, herunder betydningen af de to grundlæggende kriterier "struktureret" og "tilgængelig efter bestemte kriterier" i definitionen.

Det må på den anførte baggrund, ifølge Registerudvalget, antages, at direktivet opstiller nogle ganske rummelige "rammer", inden for hvilke det overlades til medlemsstaterne selv at fastlægge indholdet af det manuelle registerbegreb. Ifølge Registerudvalget er disse rammer ikke præcise, men det må dog – i lyset af det ovenstående – kunne lægges til grund, at Danmark vil kunne bestemme, at manuelle sagsakter/mapper eller samlinger heraf ikke inddrages under en fremtidig regulering af registerlovsområdet. Der lægges således i Registerudvalgets betænkning vægt på det, der er anført i præambelbetragtning nr. 27 i direktivet samt i den nævnte erklæring til Europa-Rådets mødeprotokol, der afspejler forhandlingsforløbet.

På denne baggrund foreslog Registerudvalget, at registerbegrebet fastlægges således, at det omfatter manuelle registre såsom kartotekskasser, journalkortsystemer og andre samlinger af manuelt materiale, som opbevares struktureret efter bestemte kriterier vedrørende personer for at lette adgangen til de indeholdte personoplysninger. Derimod bør begrebet, ifølge Registerudvalget, ikke omfatte manuelle sagsakter/mapper eller samlinger heraf. Den nærmere afgrænsning af registerbegrebet må efter udvalgets opfattelse finde sin løsning gennem vedkommende tilsynsmyndigheds praksis.

2.4.2.2. Datatilsynets praksis om manuelle registre

Datatilsynets praksis i forhold til manuelle registre er bl.a. omtalt i Datatilsynets Årsberetning fra 2000, hvor der opstilles følgende kriterier for, hvornår de ovennævnte samlinger af materiale skal betragtes som et manuelt register:

- For det første er det en betingelse, at materialet er struktureret efter bestemte kriterier. Strukturering kan bestå i inddeling efter f.eks. personnummer, fødselsdato, navn i alfabetisk rækkefølge, dato for udgående breve eller blot inddeling efter sagskategorier eller emneområder.

- For det andet er det en betingelse, at formålet med den strukturerede samling af materiale er at kunne finde frem til oplysninger om bestemte personer.[73]

[73] Datatilsynets årsberetning 2000, s. 24-25.

Henset til de opstillede kriterier fremgår det endvidere af årsberetningen, at diverse former for praksisoversigter såsom visdomsbøger eller medarbejderes egne ringbind og lignende med forskelligt materiale som udgangspunkt ikke vil være et register, idet formålet med at have disse som regel kun er at skabe sig overblik over praksis inden for forskellige områder eller at genfinde velegnede standardformuleringer. Ligeledes vil komplette samlinger af en myndigheds/virksomheds udgående breve som udgangspunkt ikke være at betegne som et register, idet sådanne "brevbøger" hovedsageligt vil være af arkivmæssig karakter eller anvendelse til rekonstruktion af almindelige sagsakter.

Endvidere fremgår det af årsberetningen, at eksempelvis en samling af navne og fotos af pågrebne butikstyve med det formål at nægte disse adgang til en forretning eller at holde ekstra øje med disse personer derimod vil være et register. Ligeledes vil en samling af oplysninger om personer, der er blevet pågrebet i overtrædelse af lovgivningen inden for et bestemt område, med henblik på at kunne holde øje med disse personer for at hindre/pågribe gentagelsestilfælde være et register. Fælles for disse to eksempler er, at formålet med den strukturerede samling af oplysninger netop er at kunne finde frem til oplysninger om bestemte personer.

Som et eksempel på en sag fra Datatilsynets praksis kan der peges på tilsynets sag med journalnummer 2012-311-0073, hvor tilsynet bl.a. kom frem til, at nogle patientjournaler, som SKAT havde modtaget fra politiet, ikke blev behandlet elektronisk eller i et manuelt register.

Herudover er Datatilsynets praksis i forhold til registre nærmere gennemgået i persondataloven med kommentarer[74], herunder f.eks. i forhold til såkaldte biobanker.

2.4.3. Databeskyttelsesforordningen

I databeskyttelsesforordningens artikel 4, nr. 6, defineres et *register* som enhver struktureret samling af personoplysninger, der er tilgængelig efter bestemte kriterier, hvad enten denne samling er placeret centralt eller decentralt eller er fordelt på funktionsbestemt eller geografisk grundlag.

Registerbegrebet skal – ligesom det hidtil har været tilfældet efter persondataloven – ses i sammenhæng med, at det af databeskyttelsesforordningens artikel 2, stk. 1, bl.a. fremgår, at forordningen finder anvendelse på behandling af personoplysninger, der er eller vil blive indeholdt i et register. Afgrænsningen af registerbegrebet har således – også fra når databe-

[74] Persondataloven med kommentarer (2015), s. 157 ff.

skyttelsesforordningen finder anvendelse – betydning for, om en behandling er omfattet af forordningen eller ej.

I forordningens præambelbetragtning nr. 15 fremgår, at beskyttelsen af fysiske personer bør gælde for både automatisk og manuel behandling af personoplysninger, hvis personoplysningerne er indeholdt eller vil blive indeholdt i et register. Det fremgår endvidere af betragtningen, at sagsmapper eller samlinger af sagsmapper samt deres forsider, som ikke er struktureret efter bestemte kriterier, ikke bør være omfattet af forordningens anvendelsesområde.

2.4.4. Overvejelser

Ved en sammenholdelse af persondatalovens (og databeskyttelsesdirektivets) definition af begrebet register med databeskyttelsesforordningens definition af samme begreb kan det konstateres, at ordlyden er den samme. Sætningen i forordningens præambelbetragtning nr. 15 om, at "Sagsmapper eller samlinger af sagsmapper samt deres forsider, som ikke er struktureret efter bestemte kriterier, bør ikke være omfattet af denne forordnings anvendelsesområde", svarer i al væsentlighed også til sidste led af direktivets præambelbetragtning nr. 27.

Der er således ikke holdepunkter for at antage, at retstilstanden har ændret sig.

På den baggrund må det derfor antages, at det er muligt at videreføre gældende ret i forhold til manuelle registre, når forordningen får virkning 25. maj 2018.

3. Forordningens kapitel II: Principper

3.1. Principper for behandling af personoplysninger, artikel 5 og artikel 6, stk. 4

3.1.1. Præsentation

I persondatalovens § 5 er der fastsat principper for al behandling af personoplysninger, herunder kravet om, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik.

Forordningens artikel 5 indeholder tilsvarende principper for al behandling af personoplysninger.

3.1.2. Gældende ret

3.1.2.1. Persondatalovens § 5, stk. 1

Det fremgår af persondatalovens § 5, stk. 1, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik. Denne bestemmelse er baseret på artikel 6, stk. 1, litra a, i databeskyttelsesdirektivet, hvoraf det fremgår, at medlemsstaterne fastsætter bestemmelser om, at personoplysninger skal behandles rimeligt og lovligt. Det fremgår af bemærkningerne til persondatalovens § 5, at den dataansvarlige skal behandle oplysninger i overensstemmelse med god databehandlingsskik. Heri ligger, at behandlingen skal være rimelig og lovlig.[75]

Det fremgår af præambelbetragtning nr. 38 i databeskyttelsesdirektivet, at en rimelig behandling af oplysninger forudsætter, at de registrerede kan få kendskab til en behandlings eksistens, og når der indsamles oplysninger hos dem, kan få nøjagtig og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen.

Endvidere fremgår det af forarbejderne til persondatalovens § 5, stk. 1, at det i øvrigt må overlades til tilsynsmyndigheden at udfylde den retlige standard »god databehandlingsskik«.[76] I Danmark er det primært Datatilsynet, som fastlægger, hvad der skal forstås ved god databehandlingsskik.

Datatilsynet henviser jævnligt til kravet om god databehandlingsskik i persondatalovens § 5, stk. 1, som en del af grundlaget for tilsynets afgørelser og udtalelser. Som eksempler på behandlinger, hvor kravet om god databehandlingsskik spiller en rolle, kan nævnes kravet

[75] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.
[76] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.

om forudgående information til de registrerede ved samkøring i kontroløjemed, kravet om meddelelse til personale mv. om tv-overvågning af bl.a. arbejdspladser inden overvågningen påbegyndes, restriktioner i anvendelsen af kreditoplysninger ved stillingsbesættelse samt pligt til alt efter indsigelsens karakter at notere den registrerede persons indsigelse mod registrerede oplysningers rigtighed.[77]

Endvidere vil det efter Datatilsynets praksis i tilfælde, hvor personoplysninger er kommet til uvedkommendes kendskab eller har været i risiko herfor som følge af en sikkerhedsbrist – afhængigt af de konkrete omstændigheder – følge af god databehandlingsskik, at den ansvarlige myndighed eller virksomhed efter omstændighederne skal underrette de berørte personer.

Det fremgår af Datatilsynet retningslinjer vedrørende utilsigtet offentliggørelse af personoplysninger på internettet, at det er et udslag af kravet om god databehandlingsskik, at den dataansvarlige skal søge at begrænse skaden, hvilket indbefatter fjernelse af oplysningerne fra hjemmesiden hurtigst muligt, underretning af de berørte personer om fejlen og undersøgelse af, om oplysningerne findes på søgemaskiner og i givet fald fjernelse derfra.

Det antages, at en adfærdskodeks, der f.eks. er udarbejdet af en brancheforening i samarbejde med Datatilsynet efter reglerne i persondatalovens § 74, kan være normgivende ved fastlæggelsen af, hvad der nærmere ligger i begrebet god databehandlingsskik.[78]

3.1.2.2. Persondatalovens § 5, stk. 2

Det fremgår af persondatalovens § 5, stk. 2, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål. Senere behandling af oplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, anses ikke for uforenelig med de formål, hvortil oplysningerne er indsamlet. Bestemmelsen svarer til artikel 6, stk. 1, litra b, i databeskyttelsesdirektivet.

Persondatalovens § 5, stk. 2, *1. pkt.*, er udtryk for princippet om formålsbestemthed. Kravet om, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, gælder uanset om indsamlingen sker hos den registrerede selv eller ej. Der påhviler således den dataansvarlige en ubetinget pligt til i forbindelse med indsamlingen af oplysninger at fastlægge til hvilket formål, indsamlingen finder sted. Indsamlingen af oplysninger kan ske til et eller flere formål.[79]

[77] Persondataloven med kommentarer (2015), s. 192-192.
[78] Persondataloven med kommentarer (2015), s. 196.
[79] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.

Artikel 29-gruppen har udtalt, at formålsbegrænsningen har to hovedbyggesten. For det første skal personoplysningerne være indsamlet til specificerede, udtrykkelige og saglige formål (formålsbegrænsning), og for det andet må personoplysningerne ikke blive genbehandlet til formål, der er uforenelige med det formål, som personoplysningerne oprindeligt var indsamlet til (forenelighed).[80]

Det fremgår endvidere af bemærkningerne til persondataloven, at i kravet om *udtrykkelighed* ligger, at den dataansvarlige i forbindelse med indsamlingen skal angive et formål, som er tilstrækkeligt veldefineret og velafgrænset til at skabe åbenhed og klarhed omkring behandlingen. Formålet med behandlingen af oplysningerne skal således defineres med en vis præcision.[81]

I relation til udtrykkelighedskravet fastslår Artikel 29-gruppen, at dette bevirker, at formålet skal være så åbenbart og udtrykkeligt, at det er sikret, at alle involverede har den samme utvetydige forståelse af formålene uden hensyn til kultur eller sproglige forskelligheder.[82] En generel eller vag definition/beskrivelse af formålet med behandlingen af oplysninger, f.eks. til "administration", vil ikke være tilstrækkelig til at opfylde kravet om udtrykkelighed. Derimod må en mere præcis angivelse som f.eks. "til brug for udbud af finansielle ydelser", anses for tilstrækkeligt.[83]

Det gælder endvidere, at udtrykkelighedskravet er en konsekvens af, at den dataansvarlige ikke må indsamle oplysninger, som denne ikke aktuelt har brug for, men som den dataansvarlige håber, at der senere viser sig at være behov for. Dette må heller ikke ske, selvom der er tale om oplysninger, der – af praktiske grunde, hvis man alligevel er i kontakt med den registrerede – indsamles som supplement til andre oplysninger, som der er et aktuelt formål med at indsamle.[84]

Indsamlingen af oplysninger skal ifølge bemærkningerne endvidere ske til et eller flere *saglige* formål. Dette vil bl.a. være tilfældet, hvor indsamlingen sker til administrative formål, som det ligger inden for den dataansvarliges myndigheds område at varetage. Endvidere vil privates indsamling af oplysninger, der ligger inden for den virksomhed, som de udøver, være til saglige formål.[85] Kravet om saglighed skal vurderes konkret i forhold til den enkelte offentlige myndighed, private virksomhed mv. Afgørende vil være, om ind-

[80] Artikel 29-gruppens udtalelse nr. 03/2013 om formålsbegrænsning (WP 203), s. 38.
[81] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.
[82] Artikel 29-gruppens udtalelse nr. 03/2013 om formålsbegrænsning (WP 203), s. 39.
[83] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.
[84] Persondataloven med kommentarer (2015), s. 197-198.
[85] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.

samlingen af oplysninger sigter mod at løse opgaver, som falder inden for myndighedens, virksomhedens mv. kompetenceområde eller lovlige virksomhedsområde.[86]

Der kan gennem lovgivning ske en nærmere specificering af, til hvilke formål behandling af oplysninger kan ske. I forhold til specifikationskravet ligger heri, at før, og under alle omstændigheder senest på det tidspunkt, hvor indsamlingen af personoplysninger sker, skal formålene være præcise og fuldt identificerede for at bestemme, hvilken behandling der kan foretages inden for det specificerede formål og for at sikre, at overholdelse af loven kan vurderes og databeskyttelsesgarantierne kan anvendes.[87]

Fra praksis kan nævnes en sag vedrørende behandling af personoplysninger i forbindelse med en forsikringssag, hvor en forsikringstager klagede til Datatilsynet over sit forsikringsselskabs behandling af personoplysninger i forbindelse med en videooptagelse og observationer som led i forsikringsselskabets behandling af et erstatningskrav rejst af forsikringstageren. Blandt de indsamlede oplysninger var oplysninger om klagers færden i sit hjem. Oplysningerne var ifølge det oplyste indsamlet ved, at forsikringsselskabets medarbejdere havde siddet uden for huset i en bil og iagttaget klager. Der var ifølge det oplyste ikke anvendt videokamera eller andet teknisk udstyr ved registreringen af klagers færden. Observationerne var i observationsrapporten beskrevet således: "Der var lys i huset, hvor SKL kunne ses gående rundt". Det var Datatilsynets opfattelse, at observation af klager i hjemmet på den omhandlede måde efter omstændighederne kunne være berettiget med henblik på opfyldelse af det angivne formål. Der var imidlertid ingen informationer om, hvorvidt klager foretog sig noget i huset, som kunne være relevant i forhold til at belyse klagers funktionsniveau. Datatilsynet fandt på den baggrund, at registrering i observationsrapporten af den pågældende observationsovervågning gik ud over det formål, som ligger til grund for forsikringsselskabets iværksættelse af overvågningen, og dermed ikke var forenelig med persondatalovens § 5, stk. 2.[88]

Det fremgår af persondatalovens § 5, stk. 2, *2. pkt.*, at *senere behandling* af oplysninger ikke må være uforenelig med de formål, hvortil oplysningerne er indsamlet (finalité-princippet). Bestemmelsen indebærer, at de oplysninger, som den dataansvarlige måtte indsamle, ikke frit vil kunne genbruges, videregives mv. Der vil således heller ikke frit kunne videregives oplysninger inden for f.eks. den offentlige forvaltning. I det omfang genbrug, udveksling mv. ikke er uforenelig med det eller de formål, hvortil oplysningerne

[86] Persondataloven med kommentarer (2015), s. 198.
[87] Artikel 29-gruppens udtalelse nr. 03/2013 om formålsbegrænsning (WP 203), s. 39.
[88] Sag vedrørende behandling af personoplysninger i forbindelse med forsikringssag, Datatilsynets j.nr. 2014-213-0047.

er indsamlet af den dataansvarlige, vil der dog være mulighed herfor. I hvilket omfang dette er tilfældet, vil bero på en konkret vurdering i den enkelte situation.

Artikel 29-gruppen anfører, at der skelnes mellem "forenelig" og dermed lovlig genbehandling og "uforenelig" og dermed ulovlig genbehandling. Artikel 29-gruppen anfører også, at det faktum, at genbehandling ikke må være "uforenelig", frem for at kræve at genbehandling skal være "forenelig", synes at tyde på, at lovgiver har haft intention om at indrømme den dataansvarlige fleksibilitet ved genbehandling.[89]

I vurderingen af, hvorvidt behandlingen er "uforenelig", skal alle relevante omstændigheder vurderes. Her skal der særligt lægges vægt på forholdet mellem det oprindelige formål og genbehandlingsformålet samt sammenhængen, hvori personoplysningerne er blevet indsamlet. Endvidere skal der særligt lægges vægt på en vurdering af, i hvilket omfang den registrerede med rimelighed må forvente genbehandling, typen af personoplysninger og den indflydelse genbehandlingen vil få for den registrerede samt sikkerhedsgarantier, som er vedtaget af den dataansvarlige for at sikre en rimelig behandling og for at hindre unødig indvirkning på den registrerede.[90]

Der er ikke dansk retspraksis om senere behandling af oplysninger, men Niels Fenger anfører, at der ved vurderingen af om en senere behandling er uforenelig med det oprindelige formål formentlig navnlig må lægges vægt på, i hvilken grad formålet med den nye brug af oplysningerne adskiller sig fra det formål, der blev specificeret ved oplysningernes indsamling. Herudover må det nok skulle indgå i vurderingen, om behandlingsgrundlaget skifter, om datakvaliteten forringes, og om der er tale om særligt følsomme oplysninger. Endelig har det formentlig også betydning, hvilke ulemper der vil være forbundet med – gennem en anmodning om at opnå samtykke til videregivelsen – at overlade det til den registrerede selv at afgøre, om oplysningerne må kunne anvendes til det nye formål.[91]

Fra praksis kan nævnes, at Datatilsynet i en sag tilkendegav, at det efter tilsynets praksis ikke ville være i strid med § 5, stk. 2, at videregive oplysninger fra Det Centrale Motorkøretøjsregister under Rigspolitichefen til kommunerne med henblik på udstedelse af parkeringstilladelser. Kommunerne kunne i forvejen få terminaladgang til Motorkøretøjsregistret til brug for behandling af parkeringsafgiftssager.[92]

[89] Artikel 29-gruppens udtalelse nr. 03/2013 om formålsbegrænsning (WP 203), s. 39.
[90] Artikel 29-gruppens udtalelse nr. 03/2013 om formålsbegrænsning (WP 203), s. 40.
[91] Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave, 2013, s. 786.
[92] Datatilsynets j.nr. 2001-321-0067, omtalt i Persondataloven med kommentarer (2015), s. 202.

Endvidere lagde Datatilsynet i en sag vedrørende forsvarets videregivelse af personaleoplysninger til Topdanmark til brug for markedsføring vægt på, at de videregivne oplysninger var indsamlet og blev behandlet for at administrere et ansættelsesforhold, og at videregivelse til en privat virksomhed med henblik på markedsføring ikke kunne anses som forenelig med dette formål. Datatilsynet lagde vægt på, at det ikke kunne antages at stå Forsvarets ansatte klart, at oplysninger, der afgives i forbindelse med et ansættelsesforhold, kan blive videregivet til en privat virksomhed til brug for markedsføring. Datatilsynet fandt ikke, at videregivelsen var i overensstemmelse med persondatalovens § 5.[93]

Det anføres i lov om behandling af personoplysninger med kommentarer, at behandling, f.eks. videregivelse til tredjemand, til andre formål end de formål, hvortil oplysningerne oprindelig er indsamlet, i øvrigt skal ske i overensstemmelse med de materielle behandlingsregler i §§ 6-13 i persondataloven, ligesom videregivelsen til tredjemand ikke må være uforenelig med de formål, som oplysningerne oprindeligt er indsamlet til.[94]

Derimod er persondatalovens § 5, stk. 2, ikke til hinder for, at den registrerede meddeler sit samtykke til, at de indsamlede oplysninger behandles til formål, der er uforenelige med de formål, hvortil oplysningerne oprindelig er indsamlet. En sådan situation er at sidestille med en fornyet indsamling af de pågældende oplysninger.[95]

Ifølge persondatalovens § 5, stk. 2, 2. pkt., er senere behandling af oplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, altid foreneligt med de formål, hvortil oplysningerne er indsamlet. Herved sikres det, at oplysninger, der ikke oprindelig er indsamlet med disse formål for øje, under alle omstændigheder vil kunne anvendes til senere behandling i historisk, statistisk eller videnskabeligt øjemed. En forudsætning herfor er dog, at den senere behandling alene sker til disse formål. Desuden er det en forudsætning for behandling efter bestemmelsens 2. pkt., at behandlingen har hjemmel i en af behandlingsreglerne eksempelvis § 10.

Samkøring og sammenstilling af oplysninger i kontroløjemed i den offentlige forvaltning
Samkøring er en fælles betegnelse for forskellige tekniske løsninger, som vedrører sammenkobling af oplysninger, der kommer fra forskellige registersystemer. Der kan blandt andet være tale om maskinelle overførsler, hvorved et register tilføres oplysninger fra et andet register, således at det modtagne register udvides med disse oplysninger, eller ma-

[93] Sag vedrørende forsvarets videregivelse af personaleoplysninger til brug for markedsføring, Datatilsynets j.nr. 2008-632-0034.
[94] Persondataloven med kommentarer (2015), s. 201.
[95] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.

skinelle sammenstillinger af oplysninger fra forskellige registre, hvorved der dannes et nyt uddataprodukt, eksempelvis et nyt register.[96]

Samkøring af personoplysninger *i kontroløjemed* kræver efter dansk ret særskilt lovhjemmel. Det følger af en tilkendegivelse fra Retsudvalgets flertal i betænkningen over lovforslag nr. L 50 af 16. januar 1991 om ændring af lov om offentlige myndigheders registre og tidligere praksis fra Registertilsynet, som er videreført af Datatilsynet, at der ved samkøring i kontroløjemed stilles krav om, at en sådan samkøring sker på et klart og utvetydigt retsgrundlag, hvilket i praksis vil sige på grundlag af direkte lovhjemmel, ligesom der stilles krav om, at de berørte personer har fået meddelelse om kontrollen, inden de afgiver oplysninger til myndigheden. Endvidere anførte Retsudvalgets flertal i betænkningen, at det var en forudsætning for samkøring i kontroløjemed, at myndighederne kun lader kontrolordningen tage sigte på fremtidige forhold, medmindre særlige forhold gør sig gældende.

Således anfører Datatilsynet eksempelvis i en udtalelse om strukturkommissionens betænkning, at Datatilsynet i sin praksis forudsætter, at myndigheder i forbindelse med sammenstilling og samkøring i kontroløjemed bl.a. har et klart og utvetydigt retsgrundlag at arbejde på.[97]

Ved samkøring i kontroløjemed forstås først og fremmest myndigheders samkøring/sammenstilling af oplysninger fra forskellige registre. Formålet kan være at afsløre, om en person har modtaget en ydelse, som vedkommende ikke er berettiget til. Formålet kan også være at afsløre ulovlige bopælsforhold eller i øvrigt at kontrollere de oplysninger, som borgeren har afgivet.

Som eksempel på lovhjemmel til samkøring i kontroløjemed kan nævnes § 11 a, stk. 2, i den sociale retssikkerhedslov og § 12 i lov om Udbetaling Danmark, jf. lovbekendtgørelse nr. 1507 af 6. december 2016.

Derudover følger det af persondatalovens § 45, stk. 1, nr. 4, at forinden behandling, som er omfattet af anmeldelsespligten i § 43, iværksættes, skal Datatilsynets udtalelse indhentes, når behandlingen omfatter samstilling eller samkøring af oplysninger i kontroløjemed.

3.1.2.3. Persondatalovens § 5, stk. 3

Det fremgår af persondatalovens § 5, stk. 3, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de for-

[96] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 67.
[97] Udtalelse om strukturkommissionens betænkning, Datatilsynets j.nr. 2004-122-0103.

mål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Det fremgår af bemærkningerne til persondataloven, at der med udtrykkene relevante og tilstrækkelige oplysninger sigtes til, at oplysningernes art skal svare til det formål, der tilsigtes med behandlingen. Bestemmelsen fastsætter endvidere, at den dataansvarliges behandling af oplysninger er undergivet et proportionalitetsprincip.[98]

I en sag vedrørende videregivelse af ejendomsoplysninger til Energi Randers udtalte Datatilsynet, at en kommune, der agtede at videregive oplysninger fra BBR-registret til et energiselskab via en terminaladgang, skulle træffe foranstaltninger for at sikre, at energiselskabet alene fik adgang til de oplysninger, som energiselskabet skulle anvende til brug for beregning af fjernvarmafgift.[99]

I en sag vedrørende en kommunes videregivelse af personnumre til et boligselskab udtalte Datatilsynet, at en kommune ikke burde videregive oplysninger om personnummer til et privat boligselskab i kommunikationen mellem kommunen og boligselskabet. Videregivelse af personnummer skulle ske med henblik på identifikation af lejere, der modtager boligstøtte. Lejemålsnumre var efter det oplyste tilstrækkelig identifikationsoplysning.[100]

Om kravene i persondatalovens § 5, stk. 3, er opfyldt, skal ses i sammenhæng med den konkrete situation, hvori oplysninger behandles. En afgørelse heraf vil i vidt omfang være skønsmæssig.[101]

3.1.2.4. Persondatalovens § 5, stk. 4

Det følger af persondatalovens § 5, stk. 4, at behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

Med denne bestemmelse stilles der krav til datakvaliteten i forbindelse med behandling af personoplysninger.

[98] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.
[99] Sag om videregivelse af ejendomsoplysninger til Energi Randers, Datatilsynets j.nr. 2003-323-0101.
[100] Sag om kommunes videregivelse af personnumre til boligselskab, Datatilsynets j.nr. 2003-323-0109.
[101] Persondataloven med kommentarer (2015), s. 202.

Det følger af bemærkningerne til persondataloven, at bestemmelsen fastsætter, at der skal foretages fornøden ajourføring af oplysningerne. Det fastsættes endvidere, at det påhviler den dataansvarlige at foretage fornøden kontrol for at sikre, at der ikke registreres urigtige eller vildledende oplysninger, og at der snarest muligt foretages sletning eller berigtigelse, hvis det viser sig, at der er behandlet urigtige eller vildledende oplysninger.[102]

Med kravet om ajourføring sikres det, at der påhviler den dataansvarlige en forpligtelse til om nødvendigt at foretage ajourføring af oplysninger, der viser sig forældede. I nogle situationer vil den dataansvarlige dog kunne afvente den førstkommende normale ajourføring, førend ajourføring skal finde sted. Afgørende for, hvor hurtigt ajourføring skal finde sted, er karakteren af de oplysninger, som er undergivet behandling. Er der eksempelvis tale om oplysninger, der vil kunne påføre den registrerede eller andre uoprettelig skade, bør ajourføring finde sted umiddelbart efter, at behovet er konstateret.[103]

Omfanget af den kontrol, som det efter bestemmelsen påhviler den dataansvarlige at foretage, vil ifølge bemærkningerne til persondataloven afhænge af oplysningernes karakter, deres anvendelse, indsamlingens pålidelighed og af, om oplysningerne er af betydning for en eller flere myndigheder mv. [104]

Det vil ofte være sådan i praksis, at hverken reglerne i § 5, stk. 4, eller § 37 fører til, at oplysninger, der viser sig urigtige, skal slettes. Det gælder, uanset om oplysningerne har været urigtige siden indsamlingen, eller de først er blevet det senere, fordi forholdene har ændret sig. Dette skyldes, at det ofte vil være nødvendigt for såvel offentlige myndigheder som private virksomheder mv. at kunne dokumentere det faktuelle grundlag, som en afgørelse eller anden beslutning i sin tid blev truffet på. Navnlig bør offentlige myndigheder udvise en betydelig tilbageholdenhed med helt at slette oplysninger, som på et tidspunkt har udgjort en del af det faktuelle grundlag, som en afgørelse er truffet på.[105] Offentlige myndigheder vil i sådanne tilfælde kunne berigtige oplysningerne i stedet for helt at slette dem.[106]

Denne manglende pligt for offentlige myndigheder til at slette oplysninger skyldes bl.a. journaliseringspligten i offentlighedslovens § 15. Når offentlige myndigheder skal berigtige urigtige eller vildledende oplysninger, vil det derfor ofte skulle ske ved at notere berig-

[102] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.
[103] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.
[104] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.
[105] Persondataloven med kommentarer (2015), s. 208.
[106] For nærmere herom henvises til Datatilsynet pjece "Kend din ret".

tigelsen (de korrekte oplysninger) på sagen uden at fjerne de oplysninger, der i forvejen fremgik. Det kan eventuelt ske i form af et notat, der lægges på sagen.

En egentlig sletning vil oftere kunne kræves, hvis der er tale om oplysninger, som indgår i et register eller andet informationssystem, hvorfra oplysningerne tilgår andre dataansvarlige, eventuelt via et online-system. Men også her må det efter omstændighederne accepteres, at det gennem en fortsat opbevaring af en kopi af registret i dets tidligere version eller på anden måde kan dokumenteres, hvilke faktuelle oplysninger der tidligere måtte være blevet videregivet.[107]

3.1.2.5. Persondatalovens 5, stk. 5

Det fremgår af persondatalovens § 5, stk. 5, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Persondatalovens § 5, stk. 5, bidrager til at sikre mod unødvendig ophobning af data, idet en dataophobning principielt altid indebærer en forøget risiko for krænkelse af de registrerede, f.eks. derved at oplysningerne kommer uvedkommende i hænde.[108]

Det fremgår af bemærkningerne til persondataloven, at oplysningerne ikke må opbevares i identificerbar form i længere tid end, hvad der er nødvendigt af hensyn til de formål, hvortil oplysningerne indsamles, eller i forbindelse med hvilke oplysningerne senere behandles.[109] Ifølge bemærkningerne er det ikke muligt generelt at beskrive, for hvilke tidsrum opbevaring af identificerbare oplysninger vil kunne ske. Dette må afgøres i den enkelte situation. Det forudsættes dog, at der gennem vedkommende tilsynsmyndigheds virksomhed vil blive fastsat nogle generelle kriterier for, hvor længe den dataansvarlige i almindelighed må opbevare identificerbare oplysninger.

Registerudvalget har i betænkning nr. 1345 udtalt, at det forudsættes, at der gennem Datatilsynets virksomhed etableres en praksis, som gør det muligt for forvaltningsmyndigheder at opbevare oplysninger, så længe der er et administrativt behov herfor. Ved vurderingen af dette spørgsmål vil der ofte kunne hentes støtte i særlovgivningen, idet denne kan indeholde regler herom. Under alle omstændigheder er det vigtigt, at myndighederne ikke tvinges til at slette oplysninger, der fortsat er et sagligt behov for at opbevare.[110]

[107] Persondataloven med kommentarer (2015), s. 209.
[108] Persondataloven med kommentarer (2015), s. 209.
[109] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.
[110] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 165.

Det faktum, at en anden myndighed kunne tænkes at anmode om oplysninger, som en dataansvarlig er i besiddelse af, kan ikke i sig selv begrunde en fortsat registrering.[111]

I en sag vedrørende indsigelse mod oplysninger om parkeringsafgift udtalte Datatilsynet, at Parkering-Københavns opbevaring af oplysninger om pålagte parkeringsafgifter i 5 år ikke var i strid med § 5, stk. 5. Datatilsynet lagde vægt på, at Parkering-København, som en del af den offentlige forvaltning, er underlagt forpligtelser med hensyn til opbevaring af sagsakter og registre, ligesom arkivlovgivningen stiller krav til myndigheders opretholdelse af registreringer. Datatilsynet lagde tillige vægt på, at Parkering-København kan have brug for oplysningerne i sagen til behandling af eventuelle klagesager eller til genoptagelse af parkeringssager. Datatilsynet udtalte, at det i disse tilfælde vil være nødvendigt at kunne identificere parten i sagen.[112]

I de situationer, hvor der er fastsat generelle slettefrister, følger det af Datatilsynets praksis, at der ikke af bestemmelsen i persondatalovens § 5, stk. 5, kan udledes en pligt for en dataansvarlig myndighed til løbende at gennemgå samtlige sine sager, dokumenter mv. med henblik på at sikre, at der ikke opbevares konkrete personoplysninger i strid med persondatalovens § 5, stk. 5, så længe myndigheden har procedurer, som sikrer, at der sker sletning i overensstemmelse med de fastsatte frister.

Det fremgår af It-sikkerhedstekst ST3 vedrørende sletning af personoplysninger fra Datatilsynet, at sletning af personoplysninger i praksis betyder, at personoplysninger uigenkaldeligt fjernes fra alle de lagringsmedier, hvorpå de har været lagret, og at personoplysninger på ingen måde kan genskabes. Dette gælder for samtlige lagringsmedier, der har været i anvendelse i forbindelse med den pågældende databehandling.[113]

Det fremgår endvidere, at der ofte vil findes flere kopier af de personoplysninger, som skal slettes. Ved normal drift af it-løsninger kan der f.eks. være tale om flere lagringsmedier som harddiske og flere generationer af backup-medier, der skal slettes. Den dataansvarlige skal således sikre sig, at alle kopier af personoplysningerne kan og bliver identificeret og slutteligt slettet.[114]

I forhold til opbevaring til arkivmæssige formål, skal det bemærkes, at det fremgår af persondatalovens § 14, at oplysninger, der er omfattet af denne lov, kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

[111] Omtalt i Persondataloven med kommentarer (2015), s. 210, og i sag vedrørende KL's overførsel af køreprøvesystem til en cloud-løsning Datatilsynet j.nr. 2011-631-0136.
[112] Sag om indsigelse mod oplysninger om parkeringsafgift, Datatilsynets j.nr. 2003-313-0180.
[113] Datatilsynets It-sikkerhedstekst ST3 vedrørende sletning af personoplysninger.
[114] Datatilsynets It-sikkerhedstekst ST3 vedrørende sletning af personoplysninger.

Specielt for så vidt angår spørgsmålet om arkivmæssig opbevaring henvises til reglerne i arkivlovgivningen herom. I det omfang opbevaringspligt følger af disse regler, vil opbevaring være berettiget.

3.1.3. Databeskyttelsesforordningen

Det fremgår af kommissionens oprindelige forslag til databeskyttelsesforordningen, at der i artikel 5 fastsættes principperne for behandling af personoplysninger, som svarer til principperne i artikel 6 i databeskyttelsesdirektivet. Det fremgår endvidere, at yderligere nye elementer omfatter gennemsigtighedsprincippet, præcisering af princippet om dataminimering og fastlæggelse af de dataansvarliges omfattende ansvar, herunder erstatningsansvar.

3.1.3.1. Databeskyttelsesforordningens artikel 5, stk. 1, litra a – lovlighed, rimelighed og gennemsigtighed

Det fremgår af forordningens artikel 5, stk. 1, litra a, at personoplysninger skal behandles rimeligt og på en gennemsigtig måde i forhold til den registrerede. Som noget nyt i forhold til de gældende regler, er der tilføjet en opsamlende "overskrifts-parentes" med ordlyden: («lovlighed, rimelighed og gennemsigtighed«).

Artikel 5, stk. 1, litra a, i forordningen har næsten identisk ordlyd med artikel 6, stk. 1, litra a, i databeskyttelsesdirektivet. Som anført ovenfor er persondatalovens § 5, stk. 1, baseret på databeskyttelsesdirektivet, hvorfor der må formodes at være samme indholdsmæssige betydning i bestemmelserne. Ordlyden i artikel 6, stk. 1, litra a, i databeskyttelsesdirektivet ses for så vidt angår den første del af artikel 5, stk. 1, litra a, i forordningen at have den samme ordlyd. Dette taler for, at denne del af bestemmelsen skal forstås i overensstemmelse med gældende ret, hvorfor forordningen antages at fastsætte en standard om *god databehandlingsskik*, som skal udfyldes af tilsynsmyndighederne.

Artikel 5, stk. 1, litra a, indeholder endvidere et krav om *gennemsigtighed*, som beskrives nærmere i præambelbetragtning nr. 39.

Det fremgår af præambelbetragtning nr. 39, at enhver behandling af personoplysninger bør være lovlig og rimelig. Det bør være gennemsigtigt for de pågældende fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet. Princippet om gennemsigtighed tilsiger, at enhver information og kommunikation vedrørende behandling af disse personoplysninger er lettilgængelig og letforståelig, og at der benyttes et klart og enkelt sprog. Dette princip vedrører navnlig oplysningen til de registrerede om den dataansvarliges identitet og formålene med den pågældende behandling samt yderligere oplysninger for at sikre en rimelig og gennemsigtig behandling for de berørte fysiske

personer og deres ret til at få bekræftelse og meddelelse om de personoplysninger vedrørende dem, der behandles. Fysiske personer bør gøres bekendt med risici, regler, garantier og rettigheder i forbindelse med behandling af personoplysninger og med, hvordan de skal udøve deres rettigheder i forbindelse med en sådan behandling.

Der ses ikke med artikel 5, stk. 1, litra a, at være tale om en ændring i forhold til den gældende retstilstand, idet der dog som nævnt er tilføjet et udtrykkeligt krav om gennemsigtighed i bestemmelsen. Det må således fortsat kunne indeholdes i forordningens artikel 5, stk. 1, litra a, at det overlades til tilsynsmyndigheden at fastlægge regler for *god databehandlingsskik*.

3.1.3.2. Databeskyttelsesforordningens artikel 5, stk. 1, litra b, og artikel 6, stk. 4 – formålsbegrænsning, forenelighed og uforenelighed

Det fremgår af databeskyttelsesforordningens artikel 5, stk. 1, litra b, at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål.

Ordlyden i forordningens artikel 5, stk. 1, litra b, ses at være næsten identisk med persondatalovens § 5, stk. 2, i forhold til *udtrykkeligt angivne og legitime formål*. I persondataloven tales der om *saglige formål* i stedet for *legitime formål*, men i databeskyttelsesdirektivet, som persondataloven baseres på, omtales også *legitime formål*. Der ses ikke at være indholdsmæssig forskel på ordene *saglig* og *legitim*. Der er endvidere ikke andre holdepunkter for at antage, at der med den ændrede formulering var tiltænkt en indholdsmæssig ændring. På denne baggrund ses der således ikke ud fra en ordlydsfortolkning af forordningens artikel 5, stk. 1, litra b, at være tale om en ændring i forhold til gældende ret.

Det fremgår af præambelbetragtning nr. 39, at især bør de specifikke formål med behandlingen af personoplysninger være udtrykkelige og legitime og fastlagt, når personoplysningerne indsamles.

Det fremgår af forordningens artikel 5, stk. 1, litra b, 2. led, at viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, ikke skal anses for at være uforenelig med de oprindelige formål. I bestemmelsen præciseres det, at reglen om formålsbegrænsning ikke forhindrer, at personoplysninger kan behandles, såfremt det sker i overensstemmelse med forordningens artikel 89, stk. 1.

For så vidt angår kriteriet om, at personoplysninger må viderebehandles til et formål, der *ikke er uforeneligt* med det oprindelige, udtrykkeligt angivne og legitime formål, svarer det til tilsvarende ordlyd i både databeskyttelsesdatadirektivet og persondataloven.

Forordningens artikel 5, stk. 1, litra b, suppleres af artikel 6, stk. 4. Af artikel 6, stk. 4, *1. led*, fremgår, at der kan ske behandling til et andet formål end det, som personoplysningerne er indsamlet til, når behandlingen er baseret på den registreredes samtykke, eller når behandlingen er baseret på EU-retten eller medlemsstaternes nationale ret. Af artikel 6, stk. 4, *2. led*, fremgår det, hvornår viderebehandling – under iagttagelse af nærmere angivne omstændigheder – i øvrigt anses for forenelig.

Forordningens artikel 6, stk. 4, er et supplement til vurderingen af, hvornår der efter artikel 5, stk. 1, litra b, er tale om et nyt formål, der lovligt kan anvendes til viderebehandling.

I databeskyttelsesforordningens artikel 6, stk. 4, præciseres det således, at der er *tre muligheder* for, hvornår en viderebehandling er lovlig og i overensstemmelse med artikel 5, stk. 1, litra b. En viderebehandling er således lovlig, hvis den for det *første* er baseret på (1) et samtykke til viderebehandlingen, på (2) EU-retten eller medlemsstaternes nationale ret i overensstemmelse med artikel 23, stk. 1, *eller* hvis (3) det nye formål kan anses for ikke at være uforeneligt med det oprindelige indsamlingsformål på baggrund af "forenelighedstesten" i artikel 6, stk. 4, 2. led, litra a-e.

Disse tre muligheder i artikel 6, stk. 4, for lovlig viderebehandling uddybes i det følgende.

Artikel 6, stk. 4, 1. led, fastslår således for det *første*, at behandling til et ellers uforeneligt formål kan ske på baggrund af den registreredes *samtykke*, jf. også artikel 6, stk. 1, litra a, og artikel 9, stk. 2, litra a, samt artikel 7 om betingelserne for samtykke. Det fremgår i den forbindelse af præambelbetragtning 50, 2. afsnit, 1. punktum bl.a., at når den registrerede har givet samtykke, bør den dataansvarlige kunne viderebehandle personoplysningerne uafhængigt af formålenes forenelighed.

Det kan for det *andet* udledes af artikel 6, stk. 4, 1. led, at det i *EU-retten eller medlemsstaternes nationale ret* kan bestemmes, at en behandling af personoplysninger, hvis formål er uforeneligt med det oprindelige formål, kan foretages, hvis den pågældende lov er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1.

Det fremgår i den forbindelse af præambelbetragtning 50, 1. afsnit, 5. punktum, at retsgrundlaget i EU-retten eller medlemsstaternes nationale ret for behandling af personoplysninger kan udgøre et retsgrundlag for viderebehandling.

Det fremgår endvidere af præambelbetragtning nr. 50, 2. afsnit, 1. pkt. bl.a., at når behandlingen er baseret på EU-retten eller medlemsstaternes nationale ret, som udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund med henblik på at beskytte navnlig vigtige målsætninger af generel samfundsinteresse, bør den dataansvarlige kunne viderebehandle personoplysningerne uafhængigt af formålenes forenelighed.

Det må på den baggrund antages, at det i en ny udgave af persondataloven med baggrund i forordningens artikel 6, stk. 4, 1. led, på *generel* vis kan reguleres nærmere efter hvilke betingelser, der kan behandles oplysninger til et nyt formål, der ellers ikke er foreneligt med det oprindelige formål, så længe en sådan national regulering ligger inden for rammerne af og hensynene i forordningens artikel 23, stk. 1, under forudsætning af, at de udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1. Som anført i afsnit 4.13 om begrænsninger af rettighederne efter artikel 23 ses der tilsvarende således ikke at være noget til hinder for i en generel lov at opretholde eller indføre lovgivningsmæssige foranstaltninger om begrænsninger, der eksempelvis svarer til persondatalovens §§ 30 og 32, stk. 1.

Muligheden i artikel 6, stk. 4, l. led, for nationalt at lovliggøre viderebehandling kan også ske i en dansk *særregel*. Som et specielt eksempel på en sådan regel, hvorefter viderebehandling anses for lovlig, kan nævnes sundhedslovens § 179, hvorefter den læge, der tilkaldes i anledning af dødsfald, skal afgive indberetning til politiet i en række tilfælde, bl.a. når dødsfaldet skyldes et strafbart forhold, selvmord eller ulykkestilfælde, eller når en person findes død mv.

Reglen i sundhedslovens § 179 ses at være i overensstemmelse med databeskyttelsesforordningens artikel 6, stk. 4, 1. led, idet der er tale om en dansk særregel, der er nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1, i dette tilfælde særligt af hensyn til artikel 23, stk. 1, litra d, om forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed.

Der findes i særlovgivningen en række regler, der forudsætter, at viderebehandling kan eller skal ske. Sådanne regler kan under forudsætning af, at de udgør en nødvendig og for-

holdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1, opretholdes.

Endelig og for det *tredje* indeholder forordningens artikel 6, stk. 4, et andet led, hvorefter den dataansvarlige, bl.a. på baggrund af "testen" i litra a-e, kan foretage en vurdering af, hvornår en viderebehandling er forenelig med det formål, som personoplysningerne oprindeligt blev indsamlet til.

Det fremgår således af forordningens artikel 6, stk. 4, 2. led, litra a-e, og præambelbetragtning nr. 50, 1. afsnit, 5. pkt., at for at afgøre om et andet behandlingsformål er foreneligt med det formål, som personoplysningerne oprindeligt blev indsamlet til, skal den dataansvarlige bl.a. tage hensyn til enhver forbindelse mellem det formål, som personoplysningerne er indsamlet til og formålet med den påtænkte viderebehandling, den sammenhæng, hvori personoplysningerne er blevet indsamlet, navnlig med hensyn til forholdet mellem den registrerede og den dataansvarlige, personoplysningernes art, navnlig om særlige kategorier af personoplysninger behandles, jf. artikel 9, eller om personoplysninger vedrørende straffedomme og lovovertrædelser behandles, jf. artikel 10, den påtænkte viderebehandlings mulige konsekvenser for de registrerede og tilstedeværelse af fornødne garantier, som kan omfatte kryptering eller pseudonymisering.[115]

Hvis en behandling således – på baggrund af denne "ikke-uforenelighedstest" – ikke er uforenelig med det oprindelige behandlingsformål, kan behandlingen lovligt ske på baggrund af og inden for rammerne af det oprindelige hjemmelsgrundlag f.eks. artikel 6, stk. 1, litra f. Dette kommer også til udtryk i præambelbetragtning nr. 50, 1. afsnit, 2. pkt.: "I dette tilfælde kræves der ikke andet retsgrundlag end det, der begrundede indsamlingen af personoplysningerne."

Det bemærkes, at det følger af forordningens artikel 13, stk. 3, og artikel 14, stk. 4, om oplysningspligt, at hvis den dataansvarlige agter at viderebehandle personoplysningerne til et andet formål end det, hvortil de er indsamlet, giver den dataansvarlige, forud for denne viderebehandling, den registrerede oplysninger om dette andet formål og andre relevante yderligere oplysninger, jf. henholdsvis artikel 13, stk. 2 og artikel 14, stk. 2.

Samkøring og sammenstilling af oplysninger i kontroløjemed i den offentlige forvaltning
For samkøring i kontroløjemed er der som tidligere anført særlige danske krav om, at der skal være lovhjemmel mv. Kravene fremgår som en forudsætning af en tilkendegivelse fra Retsudvalgets flertal i betænkningen over lovforslag nr. L 50 af 16. januar 1991 om æn-

[115] Denne beskrivelse ses at svare nogenlunde til den ovenfor gengivne sammenfatning fra Niels Fenger i Forvaltningsloven med kommentarer, 1. udgave, 2013, s. 786.

dring af lov om offentlige myndigheders registre og tidligere praksis fra Registertilsynet, som er videreført af Datatilsynet.

Efter databeskyttelsesforordningen er der ikke et udtrykkeligt krav om, at der skal være en direkte lovhjemmel til samkøring i kontroløjemed. Derudover fastsætter databeskyttelsesforordningen heller ikke et krav om, at tilsynsmyndighedens tilladelse skal indhentes, når der foretages samkøring af oplysninger i kontroløjemed, eller at der skal gives information til den registreredes, inden samkøringen foretages.

Databeskyttelsesdirektivet pålagde heller ikke medlemsstaterne sådanne krav.

Efter databeskyttelsesforordningen vil samkøring i kontroløjemed således skulle leve op til de almindelige principper og regler om behandling. Da samkøring i kontroløjemed per definition vil være en indgribende behandlingssituation, vil sådan behandling dog skærpe opmærksomheden på kravene i blandt andet forordningens artikel 5 om principper for behandling af personoplysninger, herunder proportionalitetsprincippet.

Når forordningen finder anvendelse den 25. maj 2018, må det dog antages, at det er muligt – i forarbejderne til en ny udgave af persondataloven – at operere med en forudsætning om, at samkøring i kontroløjemed bør have hjemmel særskilt i en lov.

3.1.3.3. Databeskyttelsesforordningens artikel 5, stk. 1, litra c – dataminimering
Det fremgår af forordningens artikel 5, stk. 1, litra c, at personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

Ordlyden i forordningens artikel 5, stk. 1, litra c, ses at være stort set identisk med ordlyden i persondatalovens § 5, stk. 3. Ud fra en ordlydsfortolkning af bestemmelserne ses der således ikke at være tiltænkt en anden indholdsmæssig betydning af forordningens artikel 5, stk. 1, litra c, end hvad der gælder efter gældende ret.

Det fremgår af præambelbetragtning nr. 39, at personoplysningerne bør være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålene med deres behandling. Dette kræver navnlig, at det sikres, at perioden for opbevaring af personoplysningerne ikke er længere end strengt nødvendigt. Personoplysninger bør kun behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde. Denne præambel ses at yde et fortolkningsbidrag til artikel 5, stk. 1, litra c, og af betragtningen fremgår et proportionalitetsprincip. Indholdet i denne betragtning antages at være i overensstemmelse med gældende ret.

3.1.3.4. Databeskyttelsesforordningens artikel 5, stk. 1, litra d – rigtighed

Det fremgår af forordningens artikel 5, stk. 1, litra d, at personoplysninger skal være korrekte og om nødvendigt ajourførte[116]; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges.

Det fremgår af præambelbetragtning nr. 39, at der bør træffes enhver rimelig foranstaltning for at sikre, at personoplysninger, som er urigtige, berigtiges eller slettes.

For så vidt angår ordlyden i forordningens artikel 5, stk. 1, litra d, i forhold til persondatalovens § 5, stk. 4, ses indholdet på baggrund af en ordlydsfortolkning stort set at være identisk. Dette skal også ses i sammenhæng med artikel 6, stk. 1, litra d, i databeskyttelsesdirektivet, som stort set har samme ordlyd som artikel 5, stk. 1, litra d, i forordningen.

Persondatalovens § 5, stk. 4, er baseret på artikel 6, stk. 1, litra d, i databeskyttelsesdirektivet.[117] Det antages ikke, at den ændrede formulering af persondatalovens § 5, stk. 4, har bevirket, at bestemmelsen har været tiltænkt et andet anvendelsesområde end artikel 6, stk. 1, litra d, i databeskyttelsesdirektivet – og hermed gældende ret. Som udgangspunkt vil forordningens artikel 5, stk. 1, litra d, derfor have samme anvendelsesområde som gældende ret.

Der er dog et par få sproglige ændringer, som det kan være relevant at vurdere. I forordningens tales om *straks slettes*, hvor der i persondataloven tales om *snarest muligt slettes*, og i databeskyttelsesdirektivet nævnes ikke noget tidsmæssigt aspekt i den sammenhæng. I den engelske version af forordningen tales om *without delay*, og i den tyske version af forordningen tales om *unverzüglich* – som kan oversættes med *uden tøven*, *omgående*, *øjeblikkelig* eller *straks*. Både den engelske og tyske version ses umiddelbart at være i overensstemmelse med den danske version og ordet *straks*.

På baggrund af en ordlydsfortolkning vurderes det, at en sletning efter forordningen vil skulle ske *straks*, hvilket formentlig vil være hurtigere end, hvad der følger af ordlyden i persondataloven – *snarest muligt slettes*. Det bemærkes, at denne del af bestemmelsen knytter sig til det forhold, at der behandles urigtige oplysninger, og sådanne oplysninger altså vil skulle slettes *straks* ifølge forordningen. Den ændrede ordlydsfortolkning vil fremover føre til, at sletning af urigtige oplysninger vil skulle ske med det samme og ikke

[116] I den engelske udgave af forordningen: "accurate and, where necessary, kept up to date."
[117] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.

blot snarest muligt. Bestemmelsens betydning må nærmere fastlægges i tilsynsmyndighedens praksis.

I persondataloven tales om *urigtige eller vildledende* oplysninger, mens der i databeskyttelsesdirektivet tales om *urigtige eller ufuldstændige*. I forordningen er ingen af disse ord nævnt, idet der blot tales om *urigtige*. Baseret alene på en ordlydsfortolkning af de forskellige bestemmelser ses der ikke at være grund til at antage, at forordningens bestemmelse har været tiltænkt et andet anvendelsesområde. Både *vildledende* og *ufuldstændige* vil kunne indeholdes i begrebet *urigtige*. Der kan således argumenteres for, at både *vildledende* og *ufuldstændige* oplysninger også vil kunne være *urigtige* oplysninger. Der er heller ikke andre fortolkningsbidrag, som skulle føre til en ændret vurdering. Hvis man endelig ser på formålet med selve persondataretten, vil det heller ikke være i overensstemmelse med formålet, såfremt det antages, at det skulle være tanken med forordningens artikel 5, stk. 1, litra d, at denne bestemmelse nu ikke længere skulle finde anvendelse på urigtige og vildledende oplysninger. Efter en samlet vurdering kan denne ændring i bestemmelsens ordlyd derfor ikke føre til en indholdsmæssig ændring, hvorfor *urigtige* må forstås i overensstemmelse med gældende ret.

Overordnet ses forordningens artikel 5, stk. 1, litra d, således at være i overensstemmelse med gældende ret – dog kan det antages, at urigtige oplysninger efter forordningen vil skulle slettes straks og dermed formentlig hurtigere, end hvad der følger af gældende ret.

3.1.3.5. Databeskyttelsesforordningens artikel 5, stk. 1, litra e – opbevaringsbegrænsning
Det fremgår af forordningens artikel 5, stk. 1, litra e, at personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder.

Efter en ordlydsfortolkning af forordningens artikel 5, stk. 1, litra e, 1. pkt., ses denne indholdsmæssigt at være identisk med persondatalovens § 5, stk. 5. Selvom sætningsopbygningen ikke er identisk, så anvendes de samme ord, hvorfor bestemmelserne ud fra en ordlydsfortolkning må fortolkes ens.

Vedrørende artikel 5, stk. 1, litra e, fremgår det af præambelbetragtning nr. 39, at for at sikre, at personoplysninger ikke opbevares i længere tid end nødvendigt, bør den dataansvarlige indføre tidsfrister for sletning eller periodisk gennemgang. Fortolkningsbidraget i betragtningen ses også at være i overensstemmelse med, hvad der følger af gældende ret.

Forordningens artikel 5, stk. 1, litra e, ses således at være i overensstemmelse med gældende ret.

Forordningens artikel 5, stk. 1, litra e, sidste led, henviser til forordningens artikel 89, stk. 1, hvorfor det præciseres, at reglen om opbevaringsbegrænsning ikke forhindrer, at personoplysninger kan behandles, såfremt det sker i overensstemmelse med forordningens artikel 89, stk. 1.

3.1.3.6. Databeskyttelsesforordningens artikel 5, stk. 1, litra f – integritet og fortrolighed
Det fremgår af forordningens artikel 5, stk. 1, litra f, at personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger.

Vedrørende artikel 5, stk. 1, litra f, fremgår det af præambelbetragtning nr. 39, at personoplysninger bør behandles på en måde, der garanterer tilstrækkelig sikkerhed og fortrolighed, herunder for at hindre uautoriseret adgang til eller anvendelse af personoplysninger eller af det udstyr, der anvendes til behandlingen.

Bestemmelsen fastlægger således et princip om behandlingssikkerhed.

I persondataloven og databeskyttelsesdirektivet er der ikke en bestemmelse, som svarer til forordningens artikel 5, stk. 1, litra f, og princippet om behandlingssikkerhed fremgår således ikke direkte heraf.

I persondatalovens kapitel 11 og i artikel 17 i databeskyttelsesdirektivet er der dog nærmere detaljerede regler omkring behandlingssikkerhed.

I forordningen præciserer artikel 32 nærmere kravene til behandlingssikkerheden i forbindelse med behandling af personoplysninger.

At der i forordningen er en bestemmelse om behandlingssikkerheden i afsnittet omkring principper for behandling ses at sende et signal til de dataansvarlige om, at behandlingssik-

kerhed skal tillægges stor betydning i forbindelse med behandling af personoplysninger efter forordningen.

3.1.3.7. Databeskyttelsesforordningens artikel 5, stk. 2 – ansvarlighed
Det fremgår af forordningens artikel 5, stk. 2, at den dataansvarlige er ansvarlig for og skal kunne *påvise*, at stk. 1 overholdes.

Det fremgår af databeskyttelsesdirektivets artikel 6, stk. 2, at det påhviler den dataansvarlige at *sikre*, at bestemmelserne i stk. 1 overholdes.

Der er ikke i præamblen til forordningen en uddybning af, hvordan artikel 5, stk. 2, skal forstås.

Med forordningens ordlyd understreges det, at den dataansvarlige har bevisbyrden for overholdelsen af principperne for behandling.

At den dataansvarlige nu skal påvise – mod tidligere at sikre – stemmer godt overens med forordningens røde tråd i øvrigt om ansvarlighed (accountability), som eksempelvis kommer til udtryk i artikel 24 om den dataansvarliges ansvar, i artikel 30 om fortegnelser over behandlingsaktiviteter, i artikel 35 om konsekvensanalyse vedrørende databeskyttelse samt i artikel 37 om reglerne om udpegning af en databeskyttelsesrådgiver.

3.1.4. Overvejelser
Vedrørende databeskyttelsesforordningens artikel 5, stk. 1, litra a, b, c og e, vil der ikke være tale om ændringer i forhold til gældende ret, hvorfor gældende ret efter den 25. maj 2018 kan videreføres.

Forordningens artikel 6, stk. 4, er som tidligere nævnt et bidrag til, hvordan forenelighed efter artikel 5, stk. 1, litra b, skal vurderes, og her vil der være tale om en tydeliggørelse i forhold til, hvornår der kan ske viderebehandling til andre formål end det oprindelige.

Artikel 5, stk. 1, litra d, ses endvidere ikke at være en ændring af gældende ret - dog kan det antages, at urigtige oplysninger efter forordningen vil skulle slettes straks og dermed formentlig hurtigere, end hvad der følger af gældende ret.

Artikel 5, stk. 1, litra f, præciserer behandlingssikkerhed som et princip for behandling af personoplysninger, men denne præcisering ses ikke umiddelbart at fastsætte selvstændige krav til datasikkerheden. At der i forordningen er en bestemmelse om behandlingssikkerheden i afsnittet omkring principper for behandling ses at sende et signal til de dataansvar-

lige om, at behandlingssikkerhed skal tillægges stor betydning i forbindelse med behandling af personoplysninger efter forordningen.

Artikel 5, stk. 2, præciserer, at det er den dataansvarlige, som skal kunne *påvise* – i modsætning til databeskyttelsesdirektivets krav om, at den dataansvarlige skal *sikre* – at behandlingsprincipperne skal overholdes, og dette ligger fint i tråd med, at der i øvrigt i forordningen generelt lægges stor vægt på ansvarlighed (accountability).

3.2. Forskning og statistik, artikel 5, stk. 1, litra b

3.2.1. Præsentation

Det retlige grundlag for behandling af personoplysninger i statistisk eller videnskabeligt øjemed efter persondataloven findes i §§ 6, 7, 8 og 11.

Herudover er der i lovens § 10, stk. 1, fastsat særlige regler, der giver mulighed for at behandle oplysninger omfattet af lovens § 7, stk. 1, og § 8, når behandlingen *udelukkende* sker i statistisk eller videnskabeligt øjemed.

Persondatalovens § 10, stk. 2, afskærer senere behandling af oplysningerne til andre formål, og efter stk. 3 må oplysninger omfattet af stk. 1 og 2 kun videregives til tredjemand efter forudgående tilladelse fra tilsynsmyndigheden.

3.2.2. Gældende ret

3.2.2.1. Grundlæggende principper

Persondatalovens § 5 fastlægger en række grundlæggende principper for den dataansvarliges behandling af personoplysninger. Disse regler giver ikke et selvstændigt retligt grundlag for at foretage en bestemt behandling af oplysninger, f.eks. indsamling, opbevaring, videregivelse mv. Hjemmel hertil skal i stedet søges i de øvrige behandlingsregler i §§ 6-13, kapitel 5-7 eller i særlovgivningen.

Det fremgår af persondatalovens § 5, stk. 2, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål. Senere behandling af oplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, anses ikke for uforenelig med de formål, hvortil oplysningerne er indsamlet.

Bestemmelsen, som er stort set identisk med formuleringen af databeskyttelsesdirektivets artikel 6, stk. 1, litra b, udtrykker princippet om formålsbestemthed (finalité-princippet) og

indebærer bl.a., at der fra f.eks. private og offentlige administrative registre eller sygehusregistre kan ske videregivelse til behandlinger, som alene finder sted i statistisk eller videnskabeligt øjemed, uden at dette vil stride imod princippet om formålsbestemthed.[118]

3.2.2.2. Retligt grundlag (hjemmel)
Det retlige grundlag for behandling af oplysninger i statistisk eller videnskabeligt øjemed kan foreligge i form af samtykke fra de registrerede. jf. persondatalovens § 6, stk. 1, nr. 1, § 7, stk. 2, nr. 1, eller § 8.

Lovens § 6, stk. 1, nr. 5, giver endvidere adgang til at behandle såkaldte almindelige, ikkefølsomme oplysninger, hvis behandlingen er nødvendig af hensynet til udførelsen af en opgave i samfundets interesse. Bestemmelsen gennemfører databeskyttelsesdirektivets artikel 7, litra e, og omfatter bl.a. behandling i statistisk, historisk eller videnskabeligt øjemed.[119]

Offentlige myndigheder kan i medfør persondatalovens § 11, stk. 1, behandle oplysninger om personnummer med henblik på entydig identifikation eller som journalnummer, herunder i forbindelse med behandling i statistisk og videnskabeligt øjemed. Efter lovens § 11, stk. 2, nr. 3, kan private dataansvarlige behandle personnumre, hvis behandlingen alene finder sted til videnskabelige eller statistiske formål. Disse regler har baggrund i direktivets artikel 7, stk. 7, hvorefter medlemsstaterne bestemmer, på hvilke betingelser et nationalt identifikationsnummer eller andre almene midler til identifikation kan gøres til genstand for behandling.

Herudover følger det af persondatalovens § 10, stk. l, at følsomme oplysninger, som er nævnt i lovens § 7, stk. 1, eller § 8, kan behandles, såfremt behandlingen *alene* finder sted med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning. Det er endvidere en betingelse, at behandlingen er nødvendig for udførelsen af statistiske eller videnskabelige undersøgelser. Hvis en behandling tillige har andre end videnskabelige eller statistiske formål, skal den vurderes efter lovens § 7 (stk. 2-7) eller § 8 (stk. 1-2 og stk. 4-5).[120]

[118] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 257f.
[119] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[120] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 10.

Denne formålsbegrænsning indebærer bl.a., at der ikke i medfør af § 10, stk. 1, kan ske behandling af oplysninger, der også sker i journalistisk øjemed[121], ligesom oplysningerne ikke kan anvendes til administrativ sagsbehandling eller patientbehandling.

Som eksempel herpå kan nævnes, at medicinalvirksomheder ikke med hjemmel i § 10, stk. 1, kan behandle personoplysninger til brug ved kliniske forsøg med lægemidler omfattet af lov om lægemidler, ved afprøvninger af medicinsk udstyr omfattet af lov om medicinsk udstyr eller i forbindelse med pligtmæssig sikkerhedsovervågning (bivirkningsrapportering) af lægemidler og medicinsk udstyr efter de nævnte to love.

Dette skyldes, at der i lægemiddellovgivningen er regler om, at Lægemiddelstyrelsen skal modtage indberetninger om bivirkninger og alvorlige uønskede hændelser mv., hvorefter oplysningerne indgår i styrelsens administrative sagsbehandling. Hjemmel til at indsamle, registrere, videregive og i øvrigt behandle personoplysninger i de nævnte sammenhænge skal derfor i stedet findes i reglerne i persondatalovens kapitel 4, som oftest i § 6 eller § 7, eller i lægemiddellovgivningen.[122]

3.2.2.2.1. Senere behandling af oplysninger omfattet af § 10, stk. 1

Det følger af persondatalovens § 10, stk. 2, at der ikke senere må ske behandling af oplysninger, som er omfattet af stk. l, til andre formål. Dette medfører bl.a., at oplysningerne heller ikke efterfølgende må anvendes til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer[123] eller anvendes i journalistisk øjemed.[124]

Der vil derfor alene kunne ske efterfølgende behandling, herunder videregivelse, jf. stk. 3, til private forskere eller offentlige myndigheder i det omfang, behandlingen udelukkende sker med henblik på udførelsen af andre statistiske eller videnskabelige undersøgelser. Det samme gælder med hensyn til behandling af andre (ikke-følsomme) oplysninger, som i henhold til § 6 alene foretages med henblik på at udføre statistiske eller videnskabelige undersøgelser.[125]

Bestemmelsen i § 10, stk. 2, åbner efter sin ordlyd ikke mulighed for, at der på grundlag af den registreredes udtrykkelige samtykke kan ske senere anvendelse eller videregivelse af oplysninger, der er behandlet i medfør af § 10, stk. 1, til brug for andre formål end forsk-

[121] Datatilsynets afgørelse i sagen med j.nr. 2002-41-2492, der er refereret i Persondataloven med kommentarer (2015), s. 328. Sagen er endvidere omtalt i Datatilsynets årsberetning 2002, s. 36-37.
[122] Persondataloven med kommentarer (2015), s. 329 f.
[123] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 257.
[124] Datatilsynets afgørelse i sagen med j.nr. 2002-41-2492, der er refereret i Persondataloven med kommentarer (2015), s. 331. Sagen er endvidere omtalt i Datatilsynets årsberetning 2002, s. 36-37.
[125] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 10.

ning og statistik. En sådan anvendelse, til andre formål på grundlag af et samtykke, har heller ikke støtte i bestemmelsens forarbejder, hvor spørgsmålet er uomtalt. Datatilsynet har udtalt[126], at § 10, stk. 2, ikke kan suppleres med samtykkereglerne i persondataloven, idet bestemmelsen må antages udtømmende at have gjort op med mulighederne for videregivelse.

Det bemærkes herved, at forbuddet mod senere behandling i andet end statistisk eller videnskabeligt øjemed alene gælder oplysninger omfattet af § 10, stk. 1. Hvis oplysningerne er indsamlet med de registreredes samtykke i medfør af bestemmelserne herom i lovens §§ 6, 7 eller 8, finder § 10, stk. 2, ikke anvendelse. Det samme gør sig gældende i relation til tilladelseskravet i § 10, stk. 3.

3.2.2.3. Tilladelse til videregivelse

Det fremgår af persondatalovens § 10, stk. 3, at videregivelse til tredjemand kun kan ske efter forudgående tilladelse fra tilsynsmyndigheden og i givet fald kun med henblik på udførelse af andre undersøgelser i statistisk eller videnskabeligt øjemed, jf. stk. l og 2. Tilsynsmyndigheden kan stille vilkår til sikring af, at oplysningerne alene vil blive anvendt til statistiske eller videnskabelige formål samt vilkår til beskyttelse af de registreredes privatliv.

Forud for meddelelse af en videregivelsestilladelse kontrollerer Datatilsynet bl.a., om en eventuel anmeldelsespligt er iagttaget i forhold til den undersøgelse, som oplysningerne skal videregives til brug for, og om behandlingen i modtagerens projekt ifølge anmeldelsen sker udelukkende i statistisk eller videnskabeligt øjemed. Der henvises til nedenstående afsnit om anmeldelse.

Datatilsynets videregivelsestilladelser tager udgangspunkt i et sæt standardiserede vilkår. Ved tilladelse til at videregive oplysninger til dataansvarlige i andre medlemsstater stiller tilsynet normalt vilkår om, at oplysningerne videregives i en form, hvor de ikke er umiddelbart personhenførbare for modtageren (pseudonymisering). Hvis modtager er i Danmark, stilles der vilkår om pseudonymisering "i videst muligt omfang". Der gives som altovervejende udgangspunkt ikke tilladelse til at videregive oplysninger til dataansvarlige i tredjelande.

Siden medio 2015 har Datatilsynet i medfør af § 10, stk. 3, generelle videregivelsestilladelser til offentlige myndigheder, der behandler oplysninger på baggrund af § 10, stk. 1. Videregivelse fra private (forskere, forskningsinstitutioner m.fl.) samt videregivelse fra offent-

[126] Datatilsynets j.nr. 2002-216-0096, sagen er refereret i tilsynets årsberetning 2002, s. 68-69.

lige myndigheder til dataansvarlige i udlandet eller af biologisk materiale fra manuelle registre (biobanker) kræver dog fortsat individuelle tilladelser.

3.2.2.4. Databeskyttelsesdirektivet

Persondatalovens § 10 har, for så vidt angår oplysninger omfattet af § 7, stk. 1, sin baggrund i databeskyttelsesdirektivets artikel 8, stk. 4, hvorefter medlemsstaterne med forbehold af, at der gives tilstrækkelige garantier, af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, kan fastsætte andre undtagelser fra forbuddet mod behandling af de særlige kategorier af personoplysninger, der er oplistet i direktivets artikel 8, stk. 1, end de undtagelser, som følger af artikel 8, stk. 2, enten ved national lovgivning eller ved en afgørelse truffet af tilsynsmyndigheden.

Efter artikel 8 stk. 5, må behandling af oplysninger om lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger kun foretages under kontrol af en offentlig myndighed, eller hvis der gælder tilstrækkelige, specifikke garantier i medfør af den nationale lovgivning med forbehold af de undtagelser, som medlemsstaten kan fastsætte på grundlag af nationale lovbestemmelser, hvorefter der gives tilstrækkelige, specifikke garantier. Et fuldstændigt register over straffedomme må dog kun føres under kontrol af en offentlig myndighed.

Bestemmelserne i § 10 udgør således en særlig dansk regulering, der giver en lempeligere adgang til at behandle følsomme oplysninger end efter udgangspunktet i direktivets artikel 8, stk. 1, for så vidt angår oplysninger, der behandles udelukkende i statistisk eller videnskabeligt øjemed.

Af Registerudvalgets betænkning nr. 1345[127] fremgår, at det er udvalgets opfattelse, at der ved at stille krav om, *at* undersøgelserne skal være af væsentlig samfundsmæssig betydning, *at* behandlingen skal være nødvendig for udførelsen af undersøgelserne, samt *at* der skal indhentes tilladelse til videregivelse, opstilles de fornødne garantier mod misbrug af de behandlede oplysninger, jf. forbeholdene om tilstrækkelige garantier i direktivets artikel 8, stk. 4 og 5.

3.2.2.5. Anmeldelse til Datatilsynet

Der er pligt til at indhente en udtalelse fra Datatilsynet, inden et offentligt forskningsprojekt mv., som er omfattet af § 10, stk. 1, iværksættes, jf. § 45, stk. 1, nr. 3. Er der tale om et privat forskningsprojekt mv., skal der indhentes en egentlig tilladelse fra Datatilsynet, jf. §

[127] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 257 f.

50, stk. 1, nr. 1[128], og tilsynet kan her fastsætte nærmere vilkår i medfør af § 50, stk. 5. Anmeldelsesordningen har grundlag i databeskyttelsesdirektivets afdeling IX.

Datatilsynets vilkår for private forsknings- og statistikprojekter fastsættes med udgangspunkt i et sæt standardvilkår, som tilpasses det enkelte projekt. Vilkårene har navnlig til formål at beskytte de registrerede personer, bl.a. gennem krav til datasikkerheden i projektet, herunder stilles der vilkår om kryptering og pseudonymisering.

Der stilles også krav om, at oplysninger ikke må opbevares i personhenførbar form i længere tid, end det er nødvendigt for projektets gennemførelse. Ved projektets afslutning skal oplysningerne slettes eller anonymiseres, således at det efterfølgende ikke er muligt at identificere enkeltpersoner, der indgår i undersøgelsen. Hvis oplysningerne ønskes bevaret i personhenførbar form, kan de i stedet overføres til videre opbevaring ved Rigsarkivet efter arkivlovens regler. Det er også et vilkår, at en eventuel offentliggørelse af undersøgelsens resultater ikke må ske på en sådan måde, at det er muligt at identificere enkeltpersoner.

3.2.3. Databeskyttelsesforordningen

3.2.3.1. Grundlæggende principper

Databeskyttelsesforordningen viderefører i vidt omfang behandlingsreglerne i databeskyttelsesdirektivet, herunder de grundlæggende behandlingsprincipper i artikel 6.

For så vidt angår princippet om formålsbestemthed, der som nævnt er udmøntet i persondatalovens § 5, stk. 2, fremgår det tilsvarende af forordningens artikel 5, stk. 1, litra b, at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål ("formålsbegrænsning").

3.2.3.1.1. Retligt grundlag (hjemmel)

3.2.3.1.1.1. Betingelser for lovlig behandling af oplysninger

Det fremgår af forordningens artikel 6, stk. 1, at behandling kun er lovlig, hvis og i det omfang mindst ét af de oplistede forhold gør sig gældende, herunder hvis den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke

[128] Visse private undersøgelser er ved bekendtgørelse om ændring af bekendtgørelse om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for en privat dataansvarlig, jf. bekendtgørelse nr. 410 af 9. maj 2012, fritaget fra anmeldelses- og tilladelseskravet.

formål (litra a), eller hvis behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse (litra e).

Efter stk. 2 kan medlemsstaterne opretholde eller indføre mere specifikke bestemmelser for at tilpasse anvendelsen af forordningens bestemmelser om behandling med henblik på overholdelse af bl.a. litra e ved at fastsætte mere præcist specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling, herunder for andre specifikke databehandlingssituationer som omhandlet i kapitel IX (f.eks. artikel 89 om garantier og undtagelser i forbindelse med behandling til bl.a. videnskabelige eller historiske forskningsformål eller til statistiske formål).

Det fremgår af forordningens artikel 6, stk. 3, at grundlaget for behandling i henhold til bl.a. stk. 1, litra e, skal fremgå af EU-retten eller af medlemsstaternes nationale ret, som den dataansvarlige er underlagt. Formålet med behandlingen skal være fastlagt i dette retsgrundlag eller for så vidt angår den behandling, der er omhandlet i stk. 1, litra e, være nødvendig for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Det fremgår videre, at dette retsgrundlag kan indeholde specifikke bestemmelser med henblik på at tilpasse anvendelsen af bestemmelserne i forordningen, bl.a. de generelle betingelser for lovlighed af den dataansvarliges behandling, hvilke typer oplysninger der skal behandles, berørte registrerede, hvilke enheder personoplysninger må videregives til, og formålet hermed, formålsbegrænsninger, opbevaringsperioder og behandlingsaktiviteter samt behandlingsprocedurer, herunder foranstaltninger til sikring af lovlig og rimelig behandling såsom i andre specifikke databehandlingssituationer som omhandlet i kapitel IX. EU-retten eller medlemsstaternes nationale ret skal opfylde et formål i samfundets interesse og stå i rimeligt forhold til det legitime mål, der forfølges.

Fastsættelse af nationale bestemmelser er bl.a. omtalt i betragtning 10 i forordningens præambel, hvoraf det fremgår, at for at sikre et ensartet og højt niveau for beskyttelse af fysiske personer og for at fjerne hindringerne for udveksling af personoplysninger inden for Unionen bør beskyttelsesniveauet for fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling af sådanne oplysninger være ensartet i alle medlemsstater. Det fremgår endvidere af betragtningen, at det bør sikres, at reglerne for beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger anvendes konsekvent og ensartet overalt i Unionen. Endelig fremgår det af betragtningen, at medlemsstaterne bør kunne opretholde eller indføre nationale bestemmelser for yderligere at præcisere anvendelsen af forordningens bestemmelser i forbindelse med behandling af personoplysninger for at overholde en retlig forpligtelse eller for at ud-

føre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Det fremgår endvidere af præambelbetragtning nr. 10, at medlemsstaterne har flere sektorspecifikke love på områder, hvor der er behov for mere specifikke bestemmelser der sammen med generel og horisontal lovgivning om databeskyttelse til gennemførelse af databeskyttelsesdirektivet. Det fremgår desuden af betragtningen, at forordningen også indeholder en manøvremargen, så medlemsstaterne kan præcisere reglerne heri, herunder for behandling af særlige kategorier af personoplysninger ("følsomme oplysninger"). Endelig fremgår det af betragtningen, at forordningen således ikke udelukker, at medlemsstaternes nationale ret fastlægger omstændighederne i forbindelse med specifikke databehandlingssituationer, herunder mere præcis fastlæggelse af de forhold, hvorunder behandling af personoplysninger er lovlig.

3.2.3.1.2. Straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger
Efter forordningens artikel 10 må behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på grundlag af artikel 6, stk. 1, kun foretages under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder.

3.2.3.1.3. Personnumre
For så vidt angår behandling af personnumre er det fastsat i forordningens artikel 87, at medlemsstaterne nærmere kan fastsætte de specifikke betingelser for behandling af et nationalt identifikationsnummer eller andre almene midler til identifikation. I så fald anvendes det nationale identifikationsnummer eller ethvert andet alment middel til identifikation udelukkende med de fornødne garantier for den registreredes rettigheder og frihedsrettigheder i henhold til denne forordning.

3.2.3.1.4. Særlige kategorier af oplysninger ("følsomme" oplysninger)
Forordningens artikel 9 regulerer behandling af særlige kategorier af personoplysninger, der i præambelbetragtning 10 og 51 er omtalt som "følsomme".

Det er fastsat i artikel 9, stk. 1, at behandling af personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt.

Efter forordningens artikel 9, stk. 2, litra j, finder behandlingsforbuddet i stk. 1 ikke anvendelse, hvis behandling er nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Artikel 9, stk. 4, angiver, at medlemsstaterne kan opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger.

Af forordningens præambelbetragtning nr. 159 om videnskabelige forskningsformål fremgår, at når personoplysninger behandles til videnskabelige forskningsformål, bør denne forordning også finde anvendelse på denne behandling. Behandlingen af personoplysninger til videnskabelige forskningsformål bør med henblik på denne forordning fortolkes bredt og f.eks. omfatte teknologisk udvikling og demonstration, grundforskning, anvendt forskning og privat finansieret forskning. Desuden bør den tage hensyn til Unionens mål om et europæisk forskningsrum, jf. artikel 179, stk. 1, i TEUF. Videnskabelige forskningsformål bør også omfatte studier, der udføres i samfundets interesse på folkesundhedsområdet. For at tage hensyn til de særlige forhold, der gør sig gældende ved behandling af personoplysninger til videnskabelige forskningsformål, bør der gælde særlige betingelser navnlig for offentliggørelse eller anden fremlæggelse af personoplysninger i forbindelse med videnskabelige forskningsformål. Hvis resultatet af videnskabelig forskning navnlig inden for sundhed giver grund til yderligere foranstaltninger i den registreredes interesse, bør de generelle regler i denne forordning finde anvendelse med henblik på disse foranstaltninger.

Om behandling til statistiske formål fremgår af betragtning nr. 162, at når personoplysninger behandles til statistiske formål, bør forordningen finde anvendelse på denne behandling. Det fremgår endvidere af betragtningen, at EU-retten eller medlemsstaternes nationale ret inden for rammerne af forordningen bør fastsætte statistisk indhold, adgangskontrol, præciseringer for behandling af personoplysninger til statistiske formål og passende foranstaltninger til at beskytte den registreredes rettigheder og frihedsrettigheder og sikre statistisk fortrolighed. Ved statistiske formål forstås enhver indsamling og behandlingen af personoplysninger, der er nødvendig for statistiske undersøgelser eller frembringelse af statistiske resultater. Endelig fremgår det af betragtningen, at disse statistiske resultater kan videreanvendes til forskellige formål, herunder videnskabelige forskningsformål. Det statistiske formål indebærer, at resultatet af behandling til statistiske formål ikke er personop-

lysninger, men aggregerede data, og at dette resultat eller personoplysningerne ikke anvendes til støtte for foranstaltninger eller afgørelser, der vedrører bestemte fysiske personer.

3.2.3.1.5. Garantier og undtagelser

Forordningens artikel 89, stk. 1, som artikel 9, stk. 2, litra j, henviser til, indeholder bestemmelser om garantier og undtagelser i forbindelse med behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål.

Efter stk. 1 skal behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål være underlagt fornødne garantier for registreredes rettigheder og frihedsrettigheder i overensstemmelse med forordningen. Disse garantier skal sikre, at der er truffet tekniske og organisatoriske foranstaltninger, især for at sikre overholdelse af princippet om dataminimering. Disse foranstaltninger kan omfatte pseudonymisering, forudsat at disse formål kan opfyldes på denne måde. Når formålene kan opfyldes ved viderebehandling, som ikke gør det muligt eller ikke længere gør det muligt at identificere de registrerede, skal formålene opfyldes på denne måde.

De nævnte garantier er bl.a. omtalt i præambelbetragtning nr. 156, hvoraf fremgår, at behandling af personoplysninger til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål bør være omfattet af fornødne garantier for den registreredes rettigheder og frihedsrettigheder i henhold til denne forordning. Herudover fremgår det af betragtningen, at disse garantier bør sikre, at der er truffet tekniske og organisatoriske foranstaltninger for især at sikre princippet om dataminimering. Det fremgår desuden af betragtningen, at viderebehandling af personoplysninger til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål skal foretages, når den dataansvarlige har vurderet muligheden for at opfylde disse formål ved at behandle oplysninger, som ikke gør det muligt eller ikke længere gør det muligt at identificere de registrerede, forudsat at de fornødne garantier foreligger (såsom f.eks. pseudonymisering af oplysninger). Endelig fremgår det af præambelbetragtningen, at medlemsstaterne bør sikre de fornødne garantier for behandling af personoplysninger til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål.

Det følger videre af artikel 89, stk. 2 og 3, at når personoplysninger behandles til arkivformål eller videnskabelige eller historiske forskningsformål eller til statistiske formål, kan EU-retten eller medlemsstaternes nationale ret fastsætte undtagelser fra de rettigheder, der er omhandlet i artikel 15, 16, 18 og 21 under iagttagelse af de betingelser og garantier, der er omhandlet i nærværende artikels stk. 1, såfremt sådanne rettigheder sandsynligvis vil

gøre det umuligt eller i alvorlig grad hindre opfyldelse af de specifikke formål, og sådanne undtagelser er nødvendige for at opfylde formålene.

Stk. 4 fastsætter, at når behandling som omhandlet i stk. 2 og 3, samtidig tjener et andet formål, anvendes undtagelser (til de registreredes rettigheder) kun på behandling til de formål, der er omhandlet i nævnte stykker.

3.2.3.2. Anmeldelse
Databeskyttelsesforordningen indeholder ikke regler svarende til direktivets afdeling IX om anmeldelse til den nationale tilsynsmyndighed.

Af præambelbetragtning nr. 89 fremgår om baggrunden herfor, at der ved databeskyttelsesdirektivet blev fastsat en generel forpligtelse til at anmelde behandlingen af personoplysninger til tilsynsmyndighederne. Det fremgår endvidere af betragtningen, at denne forpligtelse medførte en administrativ og finansiel byrde, men ikke i alle tilfælde bidrog til at forbedre beskyttelsen af personoplysninger. Herudover fremgår det af betragtningen, at en sådan vilkårlig og generel anmeldelsespligt derfor bør afskaffes og erstattes med effektive procedurer og mekanismer, som i stedet fokuserer på de typer behandlingsaktiviteter, der sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder i medfør af deres karakter, omfang, sammenhæng og formål. Endelig fremgår det af betragtningen, at sådanne typer behandlingsaktiviteter kan være aktiviteter, der navnlig indebærer brug af ny teknologi, eller aktiviteter som er af en ny slags, og hvor den dataansvarlige endnu ikke har foretaget en konsekvensanalyse vedrørende databeskyttelse, eller hvor de er blevet nødvendige på grund af den tid, der er gået siden den oprindelige behandling.

Det fremgår videre af præambelbetragtning nr. 90, at den dataansvarlige i sådanne tilfælde inden behandlingen bør foretage en konsekvensanalyse vedrørende databeskyttelse med henblik på at vurdere den høje risikos specifikke sandsynlighed og alvor under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt risikokilderne. Det fremgår endvidere af betragtningen, at konsekvensanalysen navnlig bør omfatte de foranstaltninger, garantier og mekanismer, der er planlagt til begrænsning af denne risiko, til sikring af beskyttelsen af personoplysninger og påvisning af overholdelse af denne forordning.

3.2.4. Overvejelser
Som beskrevet ovenfor fremgår det af forordningens artikel 5, stk. 1, litra b, at videregebehandling af oplysninger til bl.a. videnskabelige eller historiske forskningsformål eller til

statistiske formål i overensstemmelse med artikel 89, stk. 1, ikke skal anses for at være uforenelig med de oprindelige formål.

Oplysninger, der oprindelig er behandlet til andre formål, vil således også efter det tidspunkt, hvorfra forordningen finder anvendelse, kunne viderebehandles i statistisk eller videnskabeligt øjemed.

For så vidt angår spørgsmålet om hjemmelsgrundlag for behandling af oplysninger til videnskabelige eller historiske forskningsformål eller statistiske formål, henvises der til afsnit 10.5. om artikel 89.

3.3. Lovlig behandling af ikke-følsomme oplysninger, artikel 6, stk. 1

3.3.1. Præsentation

Persondatalovens § 6, stk. 1, vedrører, hvornår der kan ske behandling af almindelige ikke-følsomme oplysninger. Behandling af personoplysninger omfattet af lovens § 6 må alene finde sted, hvis en eller flere af betingelserne i § 6, stk. 1, nr. 1-7, er opfyldt. Det betyder, at de forskellige hjemler i stk. 1 er sidestillede, og behandling af personoplysninger er hjemlet, hvis blot én ud af de 7 hjemmelsgrundlag er opfyldt.

Forordningens artikel 6, stk. 1, indeholder en tilsvarende bestemmelse om, hvornår behandling af almindelige ikke-følsomme oplysninger må finde sted.

3.3.2. Gældende ret

Persondatalovens § 6, stk. 1, fastsætter de generelle betingelser for, hvornår behandling af oplysninger må finde sted. En personoplysning betragtes som omfattet af § 6 om almindelige ikke-følsomme oplysninger, hvis oplysningen ikke er omfattet af de særlige bestemmelser i lovens §§ 7-8 og § 11, der vedrører følsomme personoplysninger, eksempelvis om racemæssig eller etnisk baggrund, helbredsmæssige forhold og strafbare forhold samt regler om behandling af personnummer.

Behandling af personoplysninger omfattet af lovens § 6 må som anført finde sted, hvis mindst én af betingelserne i § 6, stk. 1, nr. 1-7, er opfyldt.
Persondatalovens § 6, stk. 1, bygger på artikel 7 i databeskyttelsesdirektivet.

3.3.2.1. Persondatalovens § 6, stk. 1, nr. 1

Det følger af persondatalovens § 6, stk. 1, nr. 1, at behandling af oplysninger må finde sted, hvis den registrerede har givet sit udtrykkelige samtykke hertil.

Bestemmelsen svarer stort set til artikel 7, litra a, i databeskyttelsesdirektivet, hvoraf det af præambelbetragtning nr. 30 fremgår, at for at være lovlig skal en behandling af personoplysninger bero på den registreredes samtykke.

Det fremgår af bemærkningerne til persondataloven, at behandling af oplysninger må finde sted, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Samtykkekravet skal forstås i overensstemmelse med den legale definition i persondatalovens § 3, nr. 8. Den dataansvarlige vil ikke kunne opnå stiltiende eller indirekte tilslutning til behandling af oplysninger, jf. herved også kravet om, at et samtykke skal være udtrykkeligt. Et egentligt krav om skriftlighed følger ikke af bestemmelsen. Der bør dog i videst muligt omfang søges indhentet et skriftligt samtykke fra den registrerede, idet der herved opnås klarhed omkring samtykkets rækkevidde.[129]

I det oprindelige forslag til lov om personoplysninger nr. L 82, fremsat den 30. april 1998, indeholdt lovens § 6, stk. 1, ikke ordet "udtrykkelige".

Den nuværende persondatalov indeholder som anført ordene "udtrykkelige samtykke" i § 6, stk. 1, nr. 1.

Justitsministeriet anførte, som svar på Retsudvalgets spørgsmål nr. 81 og 82 vedrørende forslag nr. L 82, om hvilken forskel der er på de to typer samtykke, henholdsvis *udtrykkeligt samtykke* og *samtykke*, at der ikke ved anvendelsen af udtrykket "samtykke" og udtrykket "udtrykkeligt samtykke" er tilsigtet en realitetsforskel. Den dataansvarlige kan således ikke opnå stiltiende eller indirekte tilslutning til behandling af personoplysninger.

Justitsministeriet anførte endvidere, at det herved bemærkes, at et samtykke skal opfylde definitionen i lovforslagets § 3, nr. 8. Herefter skal et samtykke være udtryk for "enhver frivillig, specifik og informeret tilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling."

Endelig anførte Justitsministeriet dog, at lovforslaget ville blive ændret i forbindelse med genfremsættelsen i det kommende folketingsår, således at det fremgik, at et samtykke i alle tilfælde skal være "udtrykkeligt".[130]

[129] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[130] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 82, FT 1997/98 (2. samling), bilag 35 fra Retsudvalget.

Derudover anførtes det i bilag 8 til lovforslag nr. L 44, fremsat den 8. oktober 1998, til lov om behandling af personoplysninger, vedrørende hvilke ændringer og præciseringer, der blev foretaget i forhold til lovforslag nr. L 82, fremsat den 30. april 1998, at der var foretaget ændring af reglerne i § 6, nr. 1, og at formålet med ændringen var at præcisere, at den dataansvarlige ikke kan opnå stiltiende eller indirekte tilslutning til behandling af personoplysninger.[131]

Det fremgår endvidere af bemærkningerne til persondataloven, at det ved behandling af oplysninger på baggrund af et samtykke fra en registreret person er en betingelse, at også de grundlæggende principper i persondatalovens § 5 er opfyldt. Behandlingen af oplysninger vil således bl.a. skulle være i overensstemmelse med god databehandlingsskik, jf. § 5, stk. 1, ligesom behandlingen også skal være sagligt begrundet og relevant, jf. § 5, stk. 2 og 3. Det forudsættes, at tilsynsmyndigheden ved vurderingen af, om dette er tilfældet, dels lægger vægt på, hvilken form for behandling der er tale om, dels hvilke typer af oplysninger behandlingen omfatter.[132]

For nærmere om samtykke skal der henvises til afsnit 2.3. om definitioner samt afsnit 3.5. om betingelser for samtykke i forordningen, artikel 7.

3.3.2.2. Persondatalovens § 6, stk. 1, nr. 2

Det følger af persondatalovens § 6, stk. 1, nr. 2, at behandling af oplysninger må finde sted, hvis behandlingen er nødvendig af hensyn til opfyldelse af en aftale, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en aftale.

Bestemmelsen svarer til artikel 7, litra b, i databeskyttelsesdirektivet, hvor det af præambelbetragtning nr. 30 fremgår, at for at være lovlig skal en behandling af personoplysninger være nødvendig med henblik på indgåelse eller opfyldelse af en kontrakt.

Det følger af bemærkningerne til persondataloven, at der i forbindelse med opfyldelsen af en indgået aftale med den registrerede kan ske den nødvendige behandling af bl.a. ordrer, fakturaer og lignende. Det er en betingelse, at den registrerede er aftalepart. En aftale mellem den dataansvarlige og eksempelvis den registreredes arbejdsgiver kan således ikke begrunde behandling af oplysninger om den registrerede.[133]

[131] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 44, FT 1998/99, bilag 8 fra Retsudvalget.
[132] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[133] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.

Artikel 29-gruppen har anført, at databeskyttelsesdirektivets artikel 7, litra b, for det første dækker situationer, hvor databehandlingen er nødvendig af hensyn til opfyldelsen af en kontrakt, som den registrerede er part i. Det kan f.eks. omfatte behandling af den registreredes adresse, således at varer, der er købt online, kan leveres, eller behandling af kreditkortoplysninger for at gennemføre betaling.[134]

Artikel 29-gruppen anfører endvidere, at bestemmelsen for det andet også omfatter databehandling, der finder sted, inden en kontrakt indgås. Dette omfatter prækontraktlige relationer, hvis tiltagene iværksættes på den registreredes anmodning og ikke på den dataansvarliges eller tredjemands initiativ. Hvis en person f.eks. anmoder en forretningsdrivende om at sende hende et tilbud på et produkt, er databehandling til dette formål, f.eks. opbevaring af adresseoplysninger og oplysninger om det, der er anmodet om, i en begrænset periode, tilladt på dette retlige grundlag. Hvis en person anmoder et forsikringsselskab om et tilbud på forsikring af sin bil, må forsikringsselskabet behandle de oplysninger, såsom bilens mærke og alder samt andre relevante og forholdsmæssige oplysninger, der er nødvendige for at udarbejde tilbuddet.[135]

Det fremgår tilsvarende af bemærkningerne til persondataloven, at den situation, at behandling af oplysninger er nødvendig af hensyn til gennemførelsen af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en aftale, også er omfattet af bestemmelsen, hvorfor bestemmelsen herved sikrer, at der også forud for parternes etablering af en aftale kan ske behandling af oplysninger.[136]

Aftaler om ansættelse vil også være omfattet af bestemmelsen. En arbejdsgiver – privat eller offentlig – vil derfor i eksempelvis et personaleregister kunne behandle de nødvendige oplysninger om arbejdstagerne uden disses samtykke, dels i forbindelse med selve ansættelsessituationen, dels efterfølgende af hensyn til det løbende ansættelsesforhold efter persondatalovens § 6, stk. 1, nr. 2.[137]

3.3.2.3. Persondatalovens § 6, stk. 1, nr. 3

Det følger af persondatalovens § 6, stk. 1, nr. 3, at behandling af oplysninger, må finde sted, hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.

---

[134] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 17-19.
[135] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 17-19.
[136] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[137] Persondataloven med kommentarer (2015), s. 219

Bestemmelsen svarer til artikel 7, litra c, i databeskyttelsesdirektivet, hvoraf det af præambelbetragtning nr. 30 fremgår, at for at være lovlig skal en behandling af personoplysninger være begrundet i et lovkrav.

Registerudvalget har i betænkning nr. 1345 udtalt, at udtrykket *retlig forpligtelse* efter en ren ordlydsfortolkning dækker over enhver form for retlig forpligtelse. Udvalget anfører endvidere, at uanset dette, kan det næppe antages, at udtrykket skal forstås således, at det omfatter alle former for retlige forpligtelser.[138]

Det følger af bemærkningerne til persondataloven, at udtrykket retlig forpligtelse omfatter forpligtelser, der følger af lovgivningen eller af administrative forskrifter, der er fastsat i medfør heraf. Omfattet af udtrykket er endvidere forpligtelser, der følger af internationale regler, herunder EU-retlige regler. Ligesom forpligtelser, der følger af en domstolsafgørelse eller af en afgørelse, der er truffet af en administrativ myndighed, også er omfattet.[139]

Det antages, at et andet lands lovgivning i almindelighed ikke kan danne grundlag for behandling af personoplysninger efter persondatalovens § 6, stk. 1, nr. 3.[140]

I tilfælde, hvor det ikke præcist er angivet i lovgivningen, hvilke oplysninger en myndighed må behandle i forbindelse med løsningen af dens opgaver, kan der eventuelt foreligge dobbelthjemmel til behandlingen.

I sag C-342/12, Worten, dom af 30. maj 2013, fastslog EU-Domstolen i sagen, som omhandlede behandling, herunder videregivelse, af personoplysninger i forbindelse med kontrol med overholdelse af arbejdstiden, at der i det konkrete tilfælde forelå dobbelthjemmel til en sådan behandling af personoplysninger i de direktivbestemmelser, som modsvarer henholdsvis persondatalovens § 6, stk. 1, nr. 3, og § 6, stk. 1, nr. 6.

Artikel 29-gruppen udtaler, at databeskyttelsesdirektivets artikel 7, litra c, har visse ligheder med artikel 7, litra e, idet en opgave i samfundets interesse ofte er baseret på eller udledt af en retlig bestemmelse. Artikel 29-gruppen anfører dernæst, at omfanget af artikel 7, litra c, dog er strengt begrænset.[141]

---

[138] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 235.
[139] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[140] Persondataloven med kommentarer (2015), s. 222.
[141] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 20.

Artikel 29-gruppen udtaler, at den retlige forpligtelse skal være tilstrækkelig klar med hensyn til den behandling af personoplysninger, den kræver. Af databeskyttelsesdirektivets artikel 7, litra c, følger således, at den retlige forpligtelse udtrykkeligt skal henvise til karakteren af og genstanden for databehandlingen. Den dataansvarlige må ikke have unødige skønsbeføjelser med hensyn til, hvordan den retlige forpligtelse skal overholdes.[142]

Aftaleretlige forpligtelser, som måtte påhvile den dataansvarlige, er ikke omfattet af bestemmelsen.[143]

Registerudvalget udtalte i den forbindelse i betænkning nr. 1345, at det synes tvivlsomt, om udtrykket en "retlig forpligtelse" dækker over rene aftaleretlige forpligtelser, som måtte påhvile den dataansvarlige. I givet fald vil dataansvarlige kunne tilvejebringe den fornødne hjemmel til behandling af oplysninger om den registrerede ved i kontraktsforhold gensidigt at påtage sig forpligtelser, til hvis opfyldelse behandling af oplysninger er nødvendig. Dette kunne efter udvalgets opfattelse ikke antages at være tilsigtet med bestemmelsen i litra c. Udvalget fandt derfor, at aftaleretlige forpligtelser bør holdes uden for udtrykket "retlig forpligtelse". Registerudvalget anførte således, at dette synes at stemme overens med reglen i artikel 7, litra b, hvorefter der kan ske den nødvendige behandling af hensyn til opfyldelsen af en kontrakt, som den registrerede – og ikke andre – er part i.[144]

Datatilsynet har i forlængelse heraf udtalt, at bestemmelser i overenskomster ikke kan anses for omfattet af reglen i persondatalovens § 6, stk. 1, nr. 3. Behandlingen i den konkrete sag kunne dog ske efter persondatalovens § 6, stk. 1, nr. 7.[145]

Artikel 29-gruppen udtaler, at den dataansvarlige ikke må kunne vælge, om han vil opfylde forpligtelsen eller ej. Frivillige ensidige forpligtelser og offentlig-private partnerskaber, der behandler oplysninger, der går videre end det, der kræves i henhold til loven, er således ikke omfattet af databeskyttelsesforordningens artikel 7, litra c.[146]

3.3.2.4. Persondatalovens § 6, stk. 1, nr. 4

Det følger af persondatalovens § 6, stk. 1, nr. 4, at behandling må ske, hvis den er nødvendig for at beskytte den registreredes vitale interesser.

[142] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 21.
[143] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[144] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 235.
[145] Sag vedrørende videregivelse af oplysninger om ikke-medlem til fagforening ved opsigelse, Datatilsynets j.nr. 2011-313-0474.
[146] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 21.

Bestemmelsen svarer til artikel 7, litra d, i databeskyttelsesdirektivet, hvoraf det af præambelbetragtning nr. 31 fremgår, at behandling af personoplysninger, der har til formål at beskytte et hensyn af fundamental betydning for den registreredes liv, ligeledes anses for lovlig.

Det fremgår af bemærkningerne til persondataloven, at dette bl.a. vil kunne være tilfældet, hvor den registrerede som følge af sygdom, bortrejse mv. ikke er i stand til at meddele samtykke, eller hvor behandling af oplysninger om den registrerede er af en sådan hastende karakter, at den dataansvarlige ikke har kunnet nå at indhente samtykke fra den registrerede.[147]

Af udtrykket *vitale interesser* følger, at behandlingen skal vedrøre interesser, som er af fundamental betydning for den registrerede. Dette vil bl.a. som nævnt være tilfældet, hvis den registrerede på grund af sygdom eller bortrejse er ude af stand til at meddele samtykke til en behandling, som vil sikre den registrerede mod at lide et væsentligt økonomisk tab eller i øvrigt lide væsentlig skade.[148]

Artikel 29-gruppen anfører, at udtrykket "vitale interesser" begrænser anvendelsen til livsvigtige spørgsmål eller i det mindste trusler, der kan medføre en risiko for personskade eller andre skader for den registrerede.[149]

Det faktum, at Artikel 29-gruppen anfører, at vitale interesser også kan omfatte *andre skader* for den registrerede, må eksempelvis antages at kunne være meget væsentlige økonomiske skader.

3.3.2.5. Persondatalovens § 6, stk. 1, nr. 5

Det følger af persondatalovens § 6, stk. 1, nr. 5, at behandling må ske, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse.

Bestemmelsen svarer til artikel 7, litra e, 1. led, i databeskyttelsesdirektivet, hvoraf det af præambelbetragtning nr. 30 fremgår, at behandling vil være lovlig, hvis behandlingen er begrundet i udførelsen af opgaver i almenhedens interesse.

[147] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[148] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[149] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 21.

I persondataloven har lovgiver opdelt databeskyttelsesdirektivets artikel 7, nr. e, i to numre, således at både persondatalovens § 6, stk. 1, nr. 5 og 6, baseres på artikel 7, litra e, i databeskyttelsesdirektivet.

Det fremgår af bemærkningerne til persondataloven, at det af udtrykket *opgave i samfundets interesse* følger, at der skal være tale om opgaver af almen interesse, dvs. opgaver, som er af betydning for en bredere kreds af personer. Dette vil bl.a. være tilfældet for så vidt angår behandling i statistisk, historisk eller videnskabeligt øjemed. Endvidere vil bestemmelsen finde anvendelse med hensyn til den behandling, som sker i retsinformationssystemer med henblik på at informere offentligheden om lovgivning, retspraksis mv. Også andre former for behandling vil kunne anses for at være af almen interesse. Dette gælder f.eks. større private foreningers og sammenslutningers registreringer af oplysninger, som er af interesse for en bredere kreds af personer. Det forhold, at behandling sker i et kommercielt øjemed, udelukker ikke, at behandlingen anses for at ske til varetagelse af almene interesser.[150]

Fra praksis kan nævnes Datatilsynets udtalelse til Foreningen af Danske Internetaktive Medier (FDIM) om indsamling af oplysninger i forbindelse med Gemius-undersøgelsen. Det fremgår af sagen, at Gemius på vegne af FDIM indsamlede data vedrørende internetbrugere på tre måder, nemlig ved hjælp af cookies og gennem henholdsvis et software og et cookie panel. Oplysningerne blev indsamlet med henblik på at udarbejde en generel opgørelse af de enkelte FDIM medlemmers websites og det danske internet generelt set. De opgjorte statistikker gav ifølge det oplyste ikke mulighed for at kunne identificere fysiske personer. FDIM oplyste desuden, at der på intet tidspunkt blev anvendt, herunder videregivet, personhenførbare oplysninger til markedsføringsformål. De indsamlede oplysninger anvendtes således udelukkende til udarbejdelse af statistikker og aldrig til markedsføring på personniveau. Den statistik, der blev udarbejdet på baggrund af de indsamlede oplysninger, blev alene anvendt til, at de websites, der abonnerede på statistikken, kunne dokumentere, at de havde brugere inden for en bestemt demografi. Datatilsynet lagde i sagen til grund, at FDIMs behandling af de indsamlede oplysninger udelukkende skete i statistisk øjemed og inden for rammerne af persondatalovens § 6, stk. 1, nr. 5, hvorfor behandling kunne finde sted.[151]

Fra praksis kan endvidere nævnes en anmeldelse, som Undervisningsministeriet foretog overfor Datatilsynet vedrørende digital tilmelding til og ansøgning om optagelse på uddan-

[150] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[151] Udtalelse til FDIM om indsamling af oplysninger i forbindelse med Gemius-undersøgelsen, Datatilsynets j.nr. 2009-321-0219.

nelser. Anmeldelsen vedrørte en digital optagelsesportal i forbindelse med ansøgning om optagelse på videregående uddannelser og ungdomsuddannelser. Optagelsesdatabasen skulle trække på en ny eksamensdatabase med eksamens- og karakteroplysninger fra de gymnasiale uddannelser samt et tidligere register med eksamensbeviser. I den forbindelse udtalte Datatilsynet, at selvom der ikke på nuværende tidspunkt er udtrykkelig lovhjemmel, hvorefter Undervisningsministeriet har fået pålagt denne opgave, er det naturligt, at ministeriet som den centrale myndighed på området, løser denne opgave. Tilsynet fandt på den baggrund, at iværksættelse af optagelsessystemet og eksamensdatabasen efter tilsynets opfattelse både kunne ske inden for rammerne af persondatalovens § 6, stk. 1, nr. 5, 6 og 7.[152]

3.3.2.6. Persondatalovens § 6, stk. 1, nr. 6

Det fremgår af persondatalovens § 6, stk. 1, nr. 6, at behandling kun må finde sted, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt.

Bestemmelsen svarer til artikel 7, litra e, 2. led, i databeskyttelsesdirektivet, hvoraf det af præambelbetragtning nr. 30 fremgår, at behandling vil være lovlig, hvis behandlingen er begrundet i udøvelsen af embedsmyndighed.

Det fremgår af bemærkningerne til persondatalovens § 6, stk. 1, nr. 6, at bestemmelsen primært retter sig mod behandling af oplysninger for offentlige myndigheder, der sker som led i myndighedsudøvelse. Kerneområdet for offentlig myndighedsudøvelse er udstedelse af forvaltningsakter, såsom meddelelse af afgørelser om sociale ydelser eller afgørelser om skatteansættelse. Også udførelse af opgaver, som sædvanligvis karakteriseres som faktisk forvaltningsvirksomhed, vil efter omstændighederne være omfattet af bestemmelsen. Med hensyn til domstolenes virksomhed omfatter udtrykket *offentlig myndighedsudøvelse* i hvert fald de judicielle funktioner.[153]

Artikel 29-gruppen henviser til, at bestemmelsen dækker situationer, hvor den dataansvarlige selv udøver offentlig myndighed (men ikke nødvendigvis også opfylder en retlig forpligtelse til at behandle oplysninger), og databehandlingen er nødvendig for at udøve denne myndighed. En skattemyndighed kan f.eks. indsamle og behandle en persons selvangivelse med det formål at beregne og kontrollere det beløb, der skal betales i skat. Et andet

[152] Anmeldelse vedrørende digital tilmelding til og ansøgning om optagelse på uddannelser, Datatilsynet j.nr. 2004-54-1396.
[153] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.

eksempel er lokale styringsorganer, f.eks. kommunale myndigheder, der har til opgave at drive bibliotekstjenester, skoler eller svømmehaller.[154] Det vil sige det, som efter forvaltningsretten karakteriseres som faktisk forvaltningsvirksomhed.

Det vil dog ikke være alt, hvad en forvaltningsmyndighed foretager sig, som vil falde inde under begrebet *offentlig myndighedsudøvelse*. Meget taler for at anse den del af en myndigheds virksomhed, som alene har karakter af service og rådgivning, for ikke at være omfattet af persondatalovens § 6, stk. 1, nr. 6, hvis denne opgave ikke er pålagt myndigheden efter lovgivningen, herunder f.eks. som en vejledningspligt efter forvaltningsloven er det. Det må endvidere nok også antages, at indtægtsdækket virksomhed og forsyningsvirksomhed falder uden for § 6, stk. 1, nr. 6.[155] Både for så vidt angår en myndigheds virksomhed, der vedrører service og rådgivning samt indtægtsdækket virksomhed og forsyningsvirksomhed, vil der dog normalt være hjemmel til den påtænkte behandling i eksempelvis persondatalovens § 6, stk. 1, nr. 2, vedrørende opfyldelsen af en aftale eller lovens § 6, stk. 1, nr. 5, vedrørende hensynet til udførelsen af en opgave i samfundets interesse. Dette vil eksempelvis være tilfældet, når kommuner behandler personoplysninger i forbindelse med kommuners udførelse af opgaver i medfør af de uskrevne kommunalfuldmagtsregler, herunder eksempelvis i forbindelse med tildeling af tilskud inden for kultur- og fritidsområdet, udlån af lokaler mv.

Artikel 29-gruppen anfører, at databeskyttelsesdirektivets artikel 7, litra e, potentielt har et meget bredt anvendelsesområde, og det fordrer en streng fortolkning og klar identifikation af den offentlige myndighedsudøvelse, der berettiger databehandlingen.[156] Tilsvarende fremgår det af persondataloven med kommentarer, at persondatalovens § 6, stk. 1, nr. 6, har et meget bredt anvendelsesområde i forhold til offentlige myndigheder.[157] Behandlingen skal dog være "nødvendig" af hensyn til udførelsen af en opgave, som henhører under offentlig myndighedsudøvelse.

Artikel 29-gruppen anfører, at i modsætning til artikel 7, litra c, kræver artikel 7, litra e, ikke, at den dataansvarlige handler på grundlag af en retlig forpligtelse.

Artikel 29-gruppen udtaler endvidere, at artikel 7, litra e, ligesom artikel 7, litra c, henviser til EU's lovgivning eller en medlemsstats lovgivning. På samme måde henviser *offentlig myndighedsudøvelse* til beføjelser, der er givet af EU eller en medlemsstat. Opgaver, der

[154] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 22.
[155] Persondataloven med kommentarer (2015), s. 224
[156] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 23.
[157] Persondataloven med kommentarer (2015), s. 225.

udføres i et andet lands interesse eller henhørende under offentlig myndighedsudøvelse i medfør af et andet lands lovgivning, er med andre ord ikke omfattet af anvendelsesområdet for denne bestemmelse.[158]

Det fremgår af bemærkningerne til persondataloven, at i det omfang offentlig myndighedsudøvelse påhviler en (privat) tredjemand, til hvem oplysninger om den registrerede er videregivet, følger det af bestemmelsen, at denne tredjemand kan foretage den nødvendige behandling af de modtagne oplysninger. Heri ligger, at f.eks. en privat tredjemand, der på baggrund af delegation eller efter aftale med en forvaltningsmyndighed varetager en opgave, der falder ind under udtrykket »offentlig myndighedsudøvelse«, vil kunne foretage den nødvendige indsamling mv. af oplysninger, herunder fra den registrerede, til brug for løsningen af denne opgave.

Artikel 29-gruppen udtaler, at artikel 7, litra e, også dækker situationer, hvor den dataansvarlige ikke udøver offentlig myndighed, men anmodes om at fremlægge oplysninger af en tredjemand, der udøver offentlig myndighed. En ansat ved et offentligt organ med ansvar for efterforskning af kriminalitet kan f.eks. anmode den dataansvarlige om at samarbejde i en igangværende efterforskning i stedet for at beordre den dataansvarlige til at overholde en specifik anmodning om samarbejde. Artikel 7, litra e, kan endvidere dække situationer, hvor den dataansvarlige proaktivt videregiver oplysninger til tredjemand, der udøver sådan offentlig myndighed. Dette kan f.eks. være tilfældet, når en dataansvarlig bemærker, at der er begået en lovovertrædelse, og på eget initiativ videregiver denne oplysning til de kompetente retshåndhævelsesmyndigheder, såsom eksempelvis politiet.[159]

Den dataansvarlige bør dog i disse situationer, hvor der videregives oplysninger på eget initiativ, sikre sig, at oplysningerne gives til den rette håndhævelsesmyndighed. Dette kan eksempelvis ske ved et forudgående telefonopkald eller lignende.[160]

Fra praksis, vedrørende en offentlig myndigheds behandling af oplysninger omfattet af persondatalovens § 6, stk. 1, nr. 6, kan nævnes en klagesag vedrørende SKATs behandling af personoplysninger. Her havde SKAT modtaget to sæt aftalekalendere vedrørende en behandlers patienter indeholdende § 6-oplysninger. I sagen udtalte Datatilsynet, at tilsynet ikke fandt grundlag for at tilsidesætte SKATs vurdering af, at behandlingen af oplysningerne i den omhandlede sag var nødvendig af hensyn til udførelsen af SKATs myndig-

[158] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 22.
[159] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 22-23.
[160] Datatilsynets j.nr. 2013-313-0254. Det bemærkes, at denne sag omhandler videregivelse efter persondatalovens § 8, men at dette principielt også gør sig gældende ved videregivelse efter § 6, stk. 1, nr. 6.

hedsopgaver. Tilsynet måtte konkludere, at behandlingen lå inden for rammerne af persondatalovens § 6, stk. 1, nr. 6. Datatilsynet lagde herved vægt på, at det fremgår af skatteforvaltningsloven, at told- og skatteforvaltningen udøver forvaltningen af lovgivning om skatter. Tilsynet lagde desuden vægt på det oplyste om, at oplysningerne blev anvendt til opgørelse af omsætningen i behandlerens virksomhed. Der kunne derfor ske behandling efter persondatalovens § 6, stk. 1, nr. 6.[161]

3.3.2.7. Persondatalovens § 6, stk. 1, nr. 7

Det følger af persondatalovens § 6, stk. 1, nr. 7, at behandling kan finde sted, hvis den er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse.

Bestemmelsen bygger på artikel 7, litra f, i databeskyttelsesdirektivet, hvoraf det fremgår, at behandling af personoplysninger må finde sted, hvis behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, medmindre den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes i henhold til artikel 1, stk. 1, i dette direktiv, går forud herfor.

Selvom bestemmelsen i persondataloven ikke har en identisk formulering i forhold til direktivet, er der ikke noget, som indikerer, at det har været ønsket med formuleringen af persondatalovens § 6, stk. 1, nr. 7, at tillægge bestemmelsen en anden betydning end direktivet.

Det fremgår af præambelbetragtning nr. 30 til databeskyttelsesdirektivet, at behandling vil være lovlig, hvis behandlingen er begrundet i en persons legitime interesse, medmindre den registreredes interesser, grundlæggende rettigheder og frihedsrettigheder går forud herfor.

Det fremgår af bemærkningerne til persondataloven, at behandling kan finde sted, hvis den er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse. En betingelse for at kunne anvende bestemmelsen er, at den dataansvarlige har foretaget en vurdering af, hvorvidt hensynet til den registreredes interesser overstiger

[161] Afgørelse i klagesag om SKATs behandling af personoplysninger, Datatilsynets j.nr. 2012-311-0073.

hensynet til de interesser, der ønskes forfulgt med behandlingen, og at denne vurdering falder ud til fordel for de interesser, der ønskes forfulgt.[162]

Der skal derfor foretages en konkret interesseafvejning af på den ene side en legitim interesse og hensynet til den registrerede.

Det, der er nødvendigt af hensyn til den dataansvarliges (eller tredjemands) legitime interesser, skal afvejes i forhold til den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder.[163] Der skal derfor udføres en afvejningstest. Artikel 29-gruppen anfører, at afvejningstesten omfatter en kompleks vurdering, der omfatter en række faktorer.[164]

Artikel 29-gruppen udtaler, at "interesser" og "rettigheder" bør fortolkes bredt, og at budskabet tydeligvis er, at alle den registreredes relevante interesser skal tages i betragtning.[165]

Det fremgår af bemærkningerne til persondataloven, at den dataansvarlige eller den tredjemand, til hvem oplysninger videregives, også vil kunne forfølge andre end deres egne interesser. En forudsætning herfor er dog, at der er tale om andres berettigede interesser.[166]

Bestemmelsen i persondatalovens § 6, stk. 1, nr. 7, kan anvendes af såvel offentlige som private dataansvarlige, men navnlig for private virksomheder, foreninger mv. har bestemmelsen stor praktisk betydning.[167]

I sag C-13/16, dom af 4. maj 2017, udtalte EU-Domstolen om databeskyttelsesdirektivets artikel 7, litra f, om begrebet "legitim interesse", at der ingen tvivl var om, at en tredjemands interesse i at få udleveret personoplysninger om en person, der havde forvoldt skade på vedkommendes ejendom, med henblik på at anlægge erstatningssag, kunne kvalificeres som en legitim interesse. EU-Domstolen udtalte i øvrigt også, at åbenhed, jf. sag C-92/09 og C-93/09, Volker und Markus Schecke, dom af 9. november 2010, præmis 77, og beskyttelsen af ejendom, sundhed og liv, jf. sag C-212/13, František Ryneš, dom af 11. december 2014, præmis 34, er legitime interesser.

[162] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[163] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 29.
[164] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 25.
[165] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 31.
[166] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.
[167] Persondataloven med kommentarer (2015), s. 230.

Fra Datatilsynets righoldige praksis om bestemmelsen kan nævnes en sag vedrørende behandling af personoplysninger i forbindelse med en forsikringssag, hvor en privatperson klagede over et forsikringsselskabs behandling af oplysninger om hende i forbindelse med videooptagelser, som forsikringsselskabet havde foretaget. Forsikringsselskabet havde en interesse i forhold til erstatningsfastsættelsen i forbindelse med en ulykke, som den registrerede havde været ude for. Datatilsynet udtalte, at tilsynet ikke fandt grundlag for at tilsidesætte forsikringsselskabets vurdering af, at nogle af undersøgelserne havde været nødvendige for at varetage forsikringsselskabets interesser efter persondatalovens § 6, stk. 1, nr. 7. Dog blev forsikringsselskabet kritiseret for at have indsamlet mere end, hvad der var nødvendigt, manglende opfyldelse af oplysningspligten mv.[168]

Endvidere kan nævnes en sag vedrørende Tryg-Balticas logning og kontrol af medarbejdernes brug af internettet. Sagen drejede sig om, at Tryg-Baltica foretog logning af stort set alt, hvad der foregik i selskabets edb-systemer, herunder også internetbrug. Loggen indeholdt oplysninger om dato og klokkeslæt for søgningen på internettet, IP-adressen, http-adressen samt fejlkode. I den forbindelse udtalte Datatilsynet, at efter reglen i § 6, stk. 1, nr. 7, kan behandling af oplysninger finde sted, hvis behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse. Datatilsynet fandt, at Tryg-Balticas logning såvel som eventuelle gennemgang af loggen ved mistanke om misbrug af internettet var nødvendig for, at selskabet kunne forfølge berettigede interesser - nemlig tekniske og sikkerhedsmæssige hensyn og hensynet til kontrol af brug - og at hensynet til de ansatte ikke oversteg disse interesser. Det var dog en forudsætning, at medarbejderne på forhånd på en klar og utvetydig måde var blevet informeret om logningen og den eventuelle gennemgang af loggen, jf. reglerne om oplysningspligt i persondatalovens §§ 28-29. Datatilsynet fandt på det foreliggende grundlag, at Tryg-Balticas information om logningen og den eventuelle gennemgang af loggen via levereglerne på selskabets intranet opfyldte denne forudsætning, hvorfor der kunne ske behandling efter persondatalovens § 6, stk. 1, nr. 7.[169]

Det følger af Datatilsynets praksis, at bestemmelsen for offentlige myndigheder ofte har været anvendt på det ansættelsesretlige område. Eksempelvis kan nævnes en sag vedrørende registrering af kommunale medarbejderes brug af internettet. I sagen udtalte Datatilsynet, at registrering af medarbejderes besøg på hjemmesider kan ske i medfør af persondatalovens § 6, stk. 1, nr. 7, under forudsætning af, at det sker til udtrykkeligt angivne og sagli-

[168] Sag vedrørende behandling af personoplysninger i forbindelse med forsikringssag, Datatilsynets j.nr. 2012-213-0047.
[169] Sag vedrørende Tryg-Balticas logning og kontrol af medarbejdernes brug af internettet, Datatilsynets j.nr. 2000-631-0001.

ge spørgsmål, jf. persondatalovens § 5, stk. 2. Datatilsynet anførte, at tilsynet anså en registrering, som varetager sikkerheds- og/eller kontrolmæssige formål, som værende saglig og legitim. Endvidere udtalte tilsynet med hensyn til en gennemgang af sendt eller modtaget e-post, at ved mistanke om misbrug vil en gennemgang heraf være nødvendig for, at kommunen kan forfølge berettigede interesser, nemlig hensynet til drift, sikkerhed, genetablering og dokumentation samt hensynet til kontrol af brug, og at hensynet til de ansatte ikke overstiger denne interesse. Behandlingen ville derfor kunne ske i medfør af persondatalovens § 6, stk. 1, nr. 7.[170]

3.3.3. Databeskyttelsesforordningen

Forordningens artikel 6 fastsætter de generelle betingelser for, hvornår behandling er lovlig. Det er samtidig en forudsætning for lovlig behandling af personoplysninger, at principperne i forordningens artikel 5 overholdes.

Forordningens ses at have samme systematik som persondataloven og databeskyttelsesdirektivet, hvorefter hjemlen til behandling af oplysninger skal findes i artikel 6, såfremt oplysningerne ikke er omfattet af særlige bestemmelser i forordningen, eksempelvis artikel 9 om følsomme oplysninger.

Behandling af personoplysninger omfattet af forordningens artikel 6 er kun lovlig, hvis og i det omfang mindst ét af forholdene i artikel 6, stk. 1, litra a-f, gør sig gældende.

Herudover følger det af præambelbetragtning nr. 40, at for, at behandling kan betragtes som lovlig, bør personoplysninger behandles på grundlag af den registreredes samtykke eller et andet legitimt grundlag, der er fastlagt ved lov enten i denne forordning eller i anden EU-ret eller i medlemsstaternes nationale ret, som omhandlet i denne forordning, herunder når det er nødvendigt for overholdelse af de retlige forpligtelser, som påhviler den dataansvarlige, eller behovet for opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til foranstaltninger, der træffes på dennes anmodning forud for indgåelse af en sådan kontrakt.

3.3.3.1. Databeskyttelsesforordningens artikel 6, stk. 1, litra a

Det fremgår af forordningens artikel 6, stk. 1, litra a, at behandling er lovlig, hvis den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.

[170] Sag vedrørende registrering af medarbejderes brug af internettet, Datatilsynets j.nr. 2000-632-0001.

Den danske forståelse af samtykke for almindelige oplysninger i persondatalovens § 6, stk. 1, litra a, harmonerer med det krav til samtykke, som følger af databeskyttelsesforordningens artikel 6, stk. 1, litra a. Dette underbygges også af, at det fremgår af præambelbetragtning nr. 32, 3. punktum, at tavshed, forudafkrydsede felter eller inaktivitet ikke bør udgøre samtykke. Forordningen indeholder en definition af samtykke i artikel 4, nr. 11, som svarer til persondatalovens, ligesom der i forordningen endvidere er fastsat enkelte yderligere krav til samtykke i artikel 7.

Samtykkets omfang må således fortsat skulle fortolkes som efter gældende dansk ret, hvor det netop i forbindelse med vurderingen af samtykkets gyldighed skal tillægges betydning, hvilken kategori af personoplysninger, der behandles (eksempelvis almindelige oplysninger eller følsomme oplysninger efter artikel 9, stk. 1).

Kravene efter forordningens artikel 6, stk. 1, litra a, ses derfor at være i overensstemmelse med, hvad der følger af gældende ret.

Der henvises i øvrigt til afsnit 3.5. om betingelser for samtykke i artikel 7.

3.3.3.2. Databeskyttelsesforordningens artikel 6, stk. 1, litra b
Det fremgår af forordningens artikel 6, stk. 1, litra b, at behandling er lovlig, hvis behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.

Bestemmelsen i forordningens artikel 6, stk. 1, litra b, svarer efter ordlyden til bestemmelsen i databeskyttelsesdirektivets artikel 7, litra b, og persondatalovens § 6, stk. 1, nr. 2.

Vedrørende forordningens artikel 6, stk. 1, litra b, fremgår det af præambelbetragtning nr. 44, at behandling bør anses for lovlig, når den er nødvendig i forbindelse med en kontrakt eller en påtænkt indgåelse af en kontrakt. Fortolkningsbidraget i betragtningen ses at være i overensstemmelse med, hvad der følger af gældende ret.

På denne baggrund ses forordningens artikel 6, stk. 1, litra b, således at være i overensstemmelse med gældende ret.

Ansættelsesforhold
Et ansættelsesforhold vil også være et kontraktforhold, hvorfor artikel 6, stk. 1, litra b, også vil kunne være relevant i denne forbindelse.

Særligt i forhold til det ansættelsesretlige område fremgår det bl.a. af forordningens artikel 88, stk. 1, at medlemsstaterne ved lov eller i medfør af kollektive overenskomster kan fastsætte mere specifikke bestemmelser for at sikre beskyttelse af rettighederne og frihedsrettighederne i forbindelse med behandling af arbejdstageres personoplysninger i ansættelsesforhold.

Vedrørende behandling i den ansættelsesretlige situation fremgår det endvidere af præambelbetragtning nr. 155 bl.a., at medlemsstaternes nationale ret eller kollektive overenskomster, herunder »lokalaftaler«, kan fastsætte specifikke bestemmelser om behandling af arbejdstageres personoplysninger i ansættelsesforhold.

Efter forordningens artikel 88, stk. 1, og præambelbetragtning nr. 155 synes der umiddelbart at være rum for, at det nationalt kan bestemmes, hvorledes der kan ske behandling af personoplysninger inden for det ansættelsesretlige område. For nærmere herom kan der henvises til afsnit 10.4. om ansættelsesforhold, artikel 88.

3.3.3.3. Databeskyttelsesforordningens artikel 6, stk. 1, litra c
Det fremgår af forordningens artikel 6, stk. 1, litra c, at behandling er lovlig, hvis behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.

Bestemmelsen i forordningens artikel 6, stk. 1, litra c, svarer efter ordlyden til bestemmelsen i databeskyttelsesdirektivets artikel 7, litra c, og persondatalovens § 6, stk. 1, nr. 3.

Vedrørende forordningens artikel 6, stk. 1, litra c, fremgår det af præambelbetragtning nr. 45, at hvis behandling foretages i overensstemmelse med en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, bør behandlingen have retsgrundlag i EU-retten eller medlemsstaternes nationale ret. Denne forordning indebærer ikke, at der kræves en specifik lov til hver enkelt behandling. Det kan være tilstrækkeligt med en lov som grundlag for adskillige databehandlingsaktiviteter, som baseres på en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse. Det bør også henhøre under EU-retten eller medlemsstaternes nationale ret at fastlægge formålet med behandlingen. Endvidere kan dette retsgrundlag præcisere denne forordnings generelle betingelser for lovlig behandling af personoplysninger og nærmere præcisere, hvem den dataansvarlige er, hvilken type personoplysninger der skal behandles, de berørte registrerede, hvilke enheder personoplysningerne kan videregives til, formålsbegrænsninger, opbevaringsperiode og andre foranstaltninger til at sikre lovlig og rimelig behandling.

Fortolkningsbidraget i betragtningen ses at være i overensstemmelse med, hvad der følger af gældende ret.

På denne baggrund er forordningens artikel 6, stk. 1, litra c, således i overensstemmelse med gældende ret.

Der kan i den forbindelse dog være grund til at overveje, om arbejdsmarkedets parter i kollektive overenskomster kan skabe en "retlig forpligtelse" i den forstand, hvori udtrykket er anvendt i forordningens artikel 6, stk. 1, litra c. Som nævnt ovenfor har Datatilsynet udtalt, at bestemmelser i overenskomster ikke kan anses for omfattet af reglen i persondatalovens § 6, stk. 1, nr. 3, jf. tilsynets j.nr.: 2011-313-0474.

Det fremgår dog af databeskyttelsesforordningens præambelbetragtning nr. 41, at når forordningen henviser til et retsgrundlag eller en lovgivningsmæssig foranstaltning, kræver det ikke nødvendigvis en lov, der er vedtaget af et parlament, med forbehold for krav i henhold til den forfatningsmæssige orden i den pågældende medlemsstat. Et sådant retsgrundlag eller en sådan lovgivningsmæssig foranstaltning bør imidlertid, fremgår det af præambelbetragtningen, være klar(t) og præcis(t), og anvendelse heraf bør være forudsigelig for personer, der er omfattet af dets/dens anvendelsesområde, jf. retspraksis fra EU-Domstolen og Den Europæiske Menneskerettighedsdomstol.

Kollektive overenskomster og det fagretlige konfliktløsningssystem udgør en helt central, retligt bindende ramme for organiseringen af det danske arbejdsmarked. Kollektive overenskomster er også på europæisk plan anerkendt for sin særlige status. EU's charter for grundlæggende rettigheder anerkender således i artikel 28 arbejdsmarkedets parters forhandlingsret og ret til kollektive skridt. Samtidigt ligger det fast, at EU-direktiver kan gennemføres via kollektive overenskomster for lønmodtagergrupper, der er omfattet af overenskomsten.

Det synes på den baggrund ikke på forhånd at kunne udelukkes, at kollektive overenskomster muligvis kan statuere en "retlig forpligtelse" i den forstand, hvori udtrykket er anvendt i forordningens artikel 6, stk. 1, litra c, jf. i den forbindelse også Peter Blume og Jens Kristiansen: Persondataret i ansættelsesforhold, 1. udgave, 2011, s. 189.

Det må endelig antages, at artikel 6, stk. 1, litra c, er direkte anvendelig som behandlingsgrundlag, når blot den retlige forpligtelse følger af f.eks. national ret. Brugen af artikel 6, stk. 1, litra c, som behandlingsgrundlag forudsætter således ikke en national, implementerende hjemmelslovgivning om *selve* den konkrete behandling af personoplysninger i for-

bindelse med fastlæggelsen af en retlig forpligtelse. Der henvises til afsnit 3.4. om forordningens artikel 6, stk. 2-3.

3.3.3.4. Databeskyttelsesforordningens artikel 6, stk. 1, litra d
Det fremgår af forordningens artikel 6, stk. 1, litra d, at behandling er lovlig, hvis behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.

Bestemmelsen i forordningens artikel 6, stk. 1, litra d, svarer efter ordlyden til bestemmelsen i databeskyttelsesdirektivets artikel 7, litra d, og persondatalovens § 6, stk. 1, nr. 4.

Dog er der i forordningens artikel 6, stk. 1, litra d, nu en tilføjelse, hvoraf det følger, at også nødvendigheden af en behandling for at beskytte *en anden fysisk persons vitale interesser* vil kunne gøre en behandling lovlig.

Som et eksempel på hvornår det vil være lovligt at behandle en oplysning om en person af hensyn til en anden fysisk persons vitale interesser, kan nævnes den situation, at det ikke er muligt for et hospital at komme i kontakt med en patient, som venter på et nyt organ på det tidspunkt, hvor hospitalet kommer i besiddelse af organet, hvorfor hospitalet er nødt til at behandle personoplysninger om patientens kæreste for at komme i kontakt med patienten.

Vedrørende forordningens artikel 6, stk. 1, litra d, fremgår det af præambelbetragtning nr. 46, at behandling af personoplysninger, der er nødvendig for at beskytte et hensyn af fundamental betydning for den registreredes eller en anden fysisk persons liv, ligeledes bør anses for lovlig. Behandling af personoplysninger på grundlag af en anden fysisk persons vitale interesser bør i princippet kun finde sted, hvis behandlingen tydeligvis ikke kan baseres på et andet retsgrundlag. Nogle typer behandling kan tjene både vigtige samfundsmæssige interesser og den registreredes vitale interesser, f.eks. når behandling er nødvendig af humanitære årsager, herunder med henblik på at overvåge epidemier og deres spredning eller i humanitære nødsituationer, navnlig i tilfælde af naturkatastrofer og menneskeskabte katastrofer.

Fortolkningsbidraget i betragtningen ses at være i overensstemmelse med, hvad der følger af gældende ret.

Forordningens artikel 6, stk. 1, litra d, er således i overensstemmelse med, hvad der følger af gældende ret – dog vil artikel 6, stk. 1, litra d, fremover også finde anvendelse i forbindelse med en anden persons vitale interesser, hvilket er en ændring i forhold til gældende ret.

3.3.3.5. Databeskyttelsesforordningens artikel 6, stk. 1, litra e
Det fremgår af forordningens artikel 6, stk. 1, litra e, at behandling er lovlig, hvis behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Bestemmelsen i forordningens artikel 6, stk. 1, litra e, svarer efter ordlyden som udgangspunkt til bestemmelsen i databeskyttelsesdirektivets artikel 7, litra e, og persondatalovens § 6, stk. 1, nr. 5 og 6.

Det fremgår af præambelbetragtning nr. 45, at hvis behandling foretages i overensstemmelse med en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, bør behandlingen have retsgrundlag i EU-retten eller medlemsstaternes nationale ret. Denne forordning indebærer ikke, at der kræves en specifik lov til hver enkelt behandling. Det kan være tilstrækkeligt med en lov som grundlag for adskillige databehandlingsaktiviteter, som baseres på en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse.

Fortolkningsbidraget i betragtningen ses at være i overensstemmelse med, hvad der følger af gældende ret.

Efter en ordlydsfortolkning er bestemmelsen i forordningens artikel 6, stk. 1, litra e, overordnet i overensstemmelse med gældende ret, jf. beskrivelsen ovenfor. Se dog vedrørende videregivelse til tredjemand, som har fået pålagt myndighedsudøvelse og samkøring i kontroløjemed i særskilte afsnit herom.

Det må i den forbindelse antages, at artikel 6, stk. 1, litra e, er direkte anvendelig som behandlingsgrundlag, så længe den dataansvarlige udfører en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Brugen af artikel 6, stk. 1, litra e, som behandlingsgrundlag forudsætter således ikke en national, implementerende hjemmelslovgivning om *selve* behandlingen af personoplysninger i forbindelse med udførelse af opgaver i samfundets interesse eller som led i offentlig myndighedsudøvelse.

Brugen af artikel 6, stk. 1, litra e, kræver heller ikke nødvendigvis, at opgaven, som kræver behandling af personoplysninger, udtrykkeligt i lovgivningen er pålagt myndigheden. Der

kan i den forbindelse henvises til den ovenfor omtalte udtalelse fra Datatilsynet[171], hvor tilsynet fandt det naturligt, at Undervisningsministeriet, som den centrale myndighed på området, løste en opgave vedrørende digital tilmelding til og ansøgning om optagelse på uddannelser, selvom der ikke var en udtrykkelig lovhjemmel, der pålagde ministeriet opgaven. Ministeriet kunne derfor bruge bl.a. § 6, stk. 1, nr. 5, i persondataloven om behandling, der er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse. Der henvises til afsnit 3.4. om forordningens artikel 6, stk. 2-3.

Videregivelse til tredjemand, som har fået pålagt myndighedsudøvelse
Det følger af databeskyttelsesdirektivets artikel 7, litra e, samt af persondatalovens § 6, stk. 1, nr. 6, at behandlingen må finde sted, hvis den er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige *eller en tredjemand, til hvem oplysningerne videregives*, har fået pålagt.

Databeskyttelsesforordningens artikel 6, stk. 1, litra e, har ikke en tilsvarende ordlyd vedrørende den myndighedsudøvelse, som tredjemand har fået pålagt. Der er ikke i forordningen anført, at en dataansvarlig i forbindelse med videregivelse til tredjemand vil kunne tillægge det betydning, om videregivelsen er begrundet i en myndighedsudøvelse, som er blevet pålagt denne tredjemand.

Forordningen indeholder således ikke en sådan videregivelseshjemmel. Dette ses dog reelt ikke at få nogen indholdsmæssig betydning for behandlingsreglerne.

Det må således antages, at artikel 6, stk. 1, litra e, fortsat kan bruges som hjemmelsgrundlag af en (privat) tredjemand – der har fået ansvar for offentlig myndighedsudøvelse, og til hvem oplysninger om den registrerede er videregivet – til den for myndighedsudøvelsen nødvendige behandling (indsamling mv.) af personoplysninger, da behandlingen netop henhører under "offentlig myndighedsudøvelse", jf. artikel 6, stk. 1, litra e.

Artikel 29-gruppen anfører, som gengivet ovenfor, som et eksempel på en videregivelse efter databeskyttelsesdirektivets artikel 7, litra e, den situation, hvor den dataansvarlige proaktivt videregiver oplysninger til tredjemand, der udøver offentlig myndighed. Dette kan f.eks. være tilfældet, når en dataansvarlig bemærker, at der er begået en lovovertrædelse og på eget initiativ videregiver denne oplysning til de kompetente retshåndhævelsesmyndigheder, som eksempelvis politiet.

[171] Anmeldelse vedrørende digital tilmelding til og ansøgning om optagelse på uddannelser, Datatilsynet j.nr. 2004-54-1396.

En sådan videregivelse vil efter forordningen fortsat kunne ske efter artikel 6, stk. 1, litra e, med henvisning til, at videregivelsen vil være i *samfundets interesse.* I dette eksempel er der således heller ikke brug for den selvstændige hjemmel vedrørende tredjemands myndighedsudøvelse.

3.3.3.6. Databeskyttelsesforordningens artikel 6, stk. 1, litra f, 1. afsnit
Det fremgår af forordningens artikel 6, stk. 1, litra f, 1. afsnit, at behandling er lovlig, hvis behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

For så vidt angår ordlyden i forordningens artikel 6, stk. 1, litra f, 1. afsnit, i forhold til databeskyttelsesdirektivets artikel 7, litra f, ses indholdet på baggrund af en ordlydsfortolkning stort set at være identisk. Som anført ovenfor, er persondatalovens § 6, stk. 1, nr. 7, implementeret på baggrund af databeskyttelsesdirektivets artikel 7, litra f, hvorfor persondatalovens bestemmelse ikke ses at være tiltænkt et andet anvendelsesområde end direktivets bestemmelse. Artikel 6, stk. 1, litra f, 1. afsnit, ses derfor umiddelbart at være i overensstemmelse med gældende ret.

At det nu særligt fremgår af forordningens artikel 6, stk. 1, litra f – modsat gældende ret – at der ved vurderingen af, hvorvidt den registreredes interesser og grundlæggende rettigheder går forud for den dataansvarliges legitime interesse, særligt skal lægges vægt på, om den registrerede er et barn, stemmer godt overens med forordningens røde tråd om, at børn skal nyde en særlig beskyttelse, hvilket eksempelvis kommer til udtryk i artikel 8 om betingelser for et barns samtykke i forbindelse med informationssamfundstjenester.

Det fremgår af præambelbetragtning nr. 47, at en dataansvarligs legitime interesser, herunder en dataansvarlig som personoplysninger kan videregives til, eller en tredjemands legitime interesser kan udgøre et retsgrundlag for behandling, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder går forud herfor under hensyntagen til registreredes rimelige forventninger på grundlag af deres forhold til den dataansvarlige. For eksempel kan der foreligge sådanne legitime interesser, når der er et relevant og passende forhold mellem den registrerede og den dataansvarlige, f.eks. hvis den registrerede er kunde hos eller gør tjeneste under den dataansvarlige. I alle tilfælde kræver tilstedeværelsen af en legitim interesse en nøje vurdering, herunder af om en registreret på tidspunktet for og i forbindelse med indsamling af personoplysninger med rimelighed kan forvente, at behandling med dette formål kan finde sted. Den registreredes interesser og grundlæggende rettigheder kan navnlig gå forud for den dataansvarliges interes-

ser, hvis personoplysninger behandles under omstændigheder, hvor registrerede ikke med rimelighed forventer viderebehandling. Behandling af personoplysninger, der er strengt nødvendig for at forebygge svig, udgør også en legitim interesse for den berørte dataansvarlige. Behandling af personoplysninger til direkte markedsføring kan anses for at være foretaget i en legitim interesse.

Det fremgår endvidere af præambelbetragtning nr. 48, at dataansvarlige, der indgår i en koncern eller i institutioner, som er tilknyttet et centralt organ, kan have en legitim interesse i at videregive personoplysninger inden for koncernen til interne administrative formål, herunder behandling af kunders eller medarbejderes personoplysninger. De generelle principper for overførsler af personoplysninger inden for en koncern til en virksomhed i et tredjeland forbliver uændrede.

Endelig fremgår det af præambelbetragtning nr. 49, at behandling af personoplysninger i det omfang, det er strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerhed, dvs. et nets eller et informationssystems evne til på et givet sikkerhedsniveau at kunne modstå utilsigtede hændelser eller ulovlige eller ondsindede handlinger, som kompromitterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af opbevarede eller transmitterede personoplysninger, og sikkerheden ved hermed forbundne tjenester udbudt af eller tilgængelige via sådanne net og systemer, der foretages af offentlige myndigheder, Computer Emergency Response Teams (CERT'er), Computer Security Incident Response Teams (CSIRT'er), udbydere af elektroniske kommunikationsnet og -tjenester og udbydere af sikkerhedsteknologier og -tjenester, udgør en legitim interesse for den berørte dataansvarlige. Behandlingen kan f.eks. have til formål at hindre uautoriseret adgang til elektroniske kommunikationsnet, distribution af ondsindet kode, standsning af overbelastningsangreb (»denial of service«-angreb) og beskadigelser af computersystemer og elektroniske kommunikationssystemer.

Fortolkningsbidraget i betragtningerne ses at være i overensstemmelse med, hvad der følger af gældende ret.

Forordningens artikel 6, stk. 1, litra f, 1. afsnit, ses således – udover nyskabelsen med det særlige hensyn til børn – at være i overensstemmelse med gældende ret. Bestemmelsen vil således fortsat kunne avendes som ovenfor beskrevet i afsnittet om gældende ret om persondatalovens § 6, stk. 1, nr. 7, herunder som hjemmelsgrundlag, når der på det private arbejdsmarked behandles personoplysninger i ansættelsesforhold.

Det fremgår endelig af præambelbetragtning nr. 10, at for at sikre et ensartet og højt niveau for beskyttelse af fysiske personer og for at fjerne hindringerne for udveksling af personoplysninger inden for Unionen bør beskyttelsesniveauet for fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling af sådanne oplysninger være ensartet i alle medlemsstater. Det bør sikres, at reglerne for beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger anvendes konsekvent og ensartet overalt i Unionen. Denne betragtning ses at knytte sig til den behandling, som finder sted efter bl.a. artikel 6, stk. 1, litra f. Det følger således heraf, at fortolkning af denne bestemmelse bør være ens i hele Unionen.

3.3.3.7. Databeskyttelsesforordningens artikel 6, stk. 1, litra f, 2. afsnit

Det fremgår af forordningens artikel 6, stk. 1, litra f, 2. afsnit, at første afsnit, litra f, ikke gælder for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

I persondataloven og databeskyttelsesdirektivet er der ikke en bestemmelse, som svarer til forordningens artikel 6, stk. 1, litra f, 2. afsnit. Som anført i afsnit 3.3.2.7. ovenfor, finder persondatalovens § 6, stk. 1, nr. 7, også anvendelse for offentlige myndigheder. Forordningens artikel 6, stk. 1, litra f, 2. afsnit, vil derfor være en nyskabelse i forhold til gældende ret.

Efter forordningen vil offentlige myndigheder som led i udførelsen af deres opgaver således ikke længere kunne foretage lovlig behandling af personoplysninger med henvisning til, at det er nødvendigt for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse.

Det fremgår af præambelbetragtning nr. 47, at eftersom det er op til lovgiver ved lov at fastsætte retsgrundlaget for offentlige myndigheders behandling af personoplysninger, bør dette retsgrundlag ikke gælde for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

Offentlige myndigheder har efter gældende ret ofte brugt persondatalovens § 6, stk. 1, nr. 7, som hjemmel for behandling af oplysninger. Den bestemmelse i forordningens artikel 6, stk. 1, litra f, som svarer hertil, vil som anført ikke finde anvendelse for offentlige myndigheders behandling som led i udførelse af deres opgaver. Selvom offentlige myndigheder herefter ikke længere har mulighed for lovlig behandling af personoplysninger med henvisning til, at behandlingen er nødvendig for at forfølge en legitim interesse, som led i udførelsen af deres opgaver, vil dette formentlig ikke få den store praktiske betydning. Offentlige myndigheder vil således i stedet have mulighed for at benytte andre behandlings-

hjemler i forbindelse med deres behandling, særligt forordningens artikel 6, stk. 1, litra c og e, om nødvendig behandling med henvisning til en retlig forpligtelse eller hensynet til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse.

Artikel 29-gruppen har i en udtalelse vedrørende artikel 7 i databeskyttelsesdirektivet udtalt sig omkring den – på dette tidspunkt foreslåede – ændring, hvorefter artikel 6, stk. 1, litra f, ikke finder anvendelse på behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

Artikel 29-gruppen udtaler, at forordningens artikel 6, stk. 1, litra f, 2. afsnit, fremhæver betydningen af det generelle princip om, at offentlige myndigheder som regel kun bør behandle personoplysninger som led i udførelsen af deres opgaver, hvis de ved lov har fået tildelt de fornødne beføjelser dertil.[172]

Artikel 29-gruppen udtaler endvidere, at der er visse ligheder mellem artikel 7, litra e, og artikel 7, litra f, og i nogle sammenhænge, især for offentlige myndigheder, kan artikel 7, litra e, erstatte artikel 7, litra f.[173]

Artikel 29-gruppen sammenligner den – på dette tidspunkt foreslåede – ændring i forordningens artikel 6, stk. 1, litra f, 2. afsnit, med Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, som indeholder de databeskyttelsesregler, der gælder for EU-institutioner og -organer, og som ikke indeholder en bestemmelse, der svarer til artikel 7, litra f. I betragtning nr. 27 til forordningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger fastsættes det, at behandling "af personoplysninger, som sker til udførelse af de opgaver, fællesskabsinstitutionerne og -organerne udfører i *samfundets interesse*, omfatter enhver behandling af personoplysninger, der er nødvendig af hensyn til administrationen af disse institutioner og organer og deres funktion".

Artikel 29-gruppen udtaler, at denne bestemmelse således tillader behandling af personoplysninger på grundlag af en bredt fortolket "opgave i samfundets interesse" i en lang række tilfælde, som ellers ville være omfattet af en bestemmelse svarende til artikel 7, litra f. Vi-

[172] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 28.
[173] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 24.

deovervågning af lokaler af hensyn til sikkerheden, elektronisk *overvågning af e-mailtrafik* eller *personaleevalueringer* er blot eksempler på situationer, der er omfattet af denne bredt fortolkede bestemmelse om opgaver, der udføres i samfundets interesse.[174]

Artikel 29-gruppen udtaler endvidere, at fremadrettet er det også vigtigt at bemærke, at forordningsforslaget i artikel 6, stk. 1, litra f, specifikt fastsætter, at det retlige grundlag vedrørende legitim interesse ikke gælder "for den behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver". Hvis denne bestemmelse fortolkes bredt, således at offentlige myndigheder ikke kan henholde sig til legitime interesser som retligt grundlag, skal de retlige grundlag "samfundets interesse" og "offentlig myndighedsudøvelse" i artikel 7, litra e, fortolkes på en måde, som giver de offentlige myndigheder en vis fleksibilitet, der som et minimum sikrer, at de kan forvaltes og fungere, sådan som forordningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger fortolkes i dag.[175]

Artikel 29-gruppen udtaler endelig, at den citerede sidste sætning i artikel 6, stk. 1, litra f, i forordningsforslaget alternativt kan fortolkes således, at offentlige myndigheder ikke helt udelukkes fra at henholde sig til legitime interesser som retligt grundlag. I det tilfælde skal udtrykket "behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver" i artikel 6, stk. 1, litra f, 2. afsnit, fortolkes snævert. En sådan snæver fortolkning vil betyde, at den databehandling, som disse offentlige myndigheder foretager som et led i deres forvaltning og drift, ikke er omfattet af udtrykket "behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver". Det betyder, at databehandling, der foretages som et led i disse offentlige myndigheders forvaltning og drift, stadig er mulig at basere på det retlige grundlag vedrørende legitim interesse.[176]

Som eksempler på, hvornår det potentielt vil få betydning, at en bestemmelse svarende til persondatalovens § 6, stk. 1, nr. 7, ikke længere finder anvendelse for behandling, som offentlige myndigheder foretager som led i deres opgaver, kan nævnes følgende situationer: Offentliggørelse af medarbejderoplysninger på internettet, offentliggørelse af afgørelser og postlister samt kontrolforanstaltninger i forhold til ansatte. Fremover vil behandling i sådanne situationer dog kunne vurderes ud fra de øvrige behandlingshjemler i forordningens artikel 6, stk. 1.

[174] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 24.
[175] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 24.
[176] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217), s. 24.

Eksempelvis vil offentliggørelse af medarbejderoplysninger og postlister herefter kunne ske, såfremt det er nødvendigt af hensyn til udførelsen af en opgave i samfundets interesse, jf. forordningens artikel 6, stk. 1, litra e.

Fra praksis kan nævnes en sag vedrørende offentliggørelse af oplysninger om mulig jordforurening, hvor Datatilsynet udtalte, at det var tilsynets vurdering, at Vestsjællands Amt efter § 6, stk. 1, nr. 7, og under iagttagelse af de almindelige principper i persondatalovens § 5, kunne offentliggøre oplysninger om en jordforureningskortlægning på amtets hjemmeside. Datatilsynet lagde i den forbindelse vægt på, at Vestsjællands Amts interesse i at offentliggøre de pågældende oplysninger og offentlighedens interesse i at få kendskab til muligt forurenede grunde fandtes at veje tungere end hensynet til den pågældende ejers interesse i ikke at få offentliggjort oplysninger om sin ejendom på internettet. Datatilsynet bemærkede i den forbindelse også, at det følger af den såkaldte Århus Konventions principper, at der skal være offentlighed i miljøoplysninger, og at borgerne skal have mulighed for at gøre sig bekendt med miljøoplysninger, herunder oplysninger om muligt eksisterende forureninger, ikke blot af hensyn til økonomiske interesser, men også til sundhedsmæssige interesser. Endelig tillagde Datatilsynet det vægt, at oplysningerne i forvejen var tilgængelige via aktindsigtsreglerne og derfor ikke kunne anses som fortrolige. Datatilsynet fandt imidlertid, at amtets konkrete offentliggørelse på internettet af klagerens grund som muligt forurenet ikke var i overensstemmelse med persondatalovens § 6, stk. 1, nr. 7, og principperne i persondatalovens § 5.[177]

Når forordningens artikel 6, stk. 1, litra f, 2. afsnit, fremover finder anvendelse, må vurderingen af en sådan offentliggørelse herefter kunne ske efter en afvejning af forordningens artikel 6, stk. 1, litra e, enten fordi offentliggørelse er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, ligesom de øvrige behandlingshjemler i forordningens artikel 6, stk. 1, måske også vil kunne anvendes.

Som anført ovenfor, er det ikke alle aktiviteter, en forvaltningsmyndighed foretager sig, som vil falde ind under begrebet offentlig myndighedsudøvelse efter persondatalovens § 6, stk. 1, nr. 6. I sådanne tilfælde har den dataansvarlige myndighed efter praksis i vidt omfang anvendt persondatalovens § 6, stk. 1, nr. 7, som hjemmel til behandlingen.

Det kan dog ikke antages at være hensigten med forordningen at begrænse offentlige myndigheders mulighed for at behandle personoplysninger. Det kan f.eks. ikke antages at være hensigten med forordningen, at behandling af personoplysninger i forbindelse med drift af

[177] Sag vedrørende offentliggørelse af oplysninger om mulig jordforurening, Datatilsynets j.nr. 2003-322-0044.

biblioteker, skoler og svømmehaller eller håndtering af personalemæssige forhold – og anden form for faktisk forvaltningsvirksomhed – ikke skulle være omfattet af forordningens behandlingshjemler. Forordningen må således kunne udgøre hjemmel, når kommuner behandler personoplysninger i forbindelse med kommuners udførelse af opgaver i medfør af de uskrevne kommunalfuldmagtsregler, herunder eksempelvis i forbindelse med tildeling af tilskud inden for kultur- og fritidsområdet, udlån af lokaler mv., men også når andre myndigheder end kommuner udfører opgaver, der naturligt falder inden for deres ressortområde, jf. Datatilsynet udtalelse i sag 2004-54-1396, som nævnt ovenfor.

Forordningen må i det hele taget også kunne udgøre hjemmel, når offentlige myndigheder indhenter oplysninger i overensstemmelse med officialmaksimen, jf. artikel 6, stk. 1, litra e. Det bemærkes i den forbindelse, at det af punkt 199 i vejledning nr. 11740/1986 om forvaltningsloven vedrørende officialmaksimen fremgår, at det er et helt grundlæggende princip i dansk forvaltningsret, at det påhviler den enkelte forvaltningsmyndighed selv, eventuelt i samarbejde med andre myndigheder, at fremskaffe fornødne oplysninger om de foreliggende sager eller dog at foranledige, at private, navnlig parterne, yder medvirken til sagens oplysning. Det bemærkes endvidere, at pligten til at medvirke til sagens oplysning i visse tilfælde er fastsat ved lov. En sådan pligt er bl.a. fastsat i den sociale retssikkerhedslovs §§ 11 a og 11 c, som myndigheder har pligt til at oplyse borgeren om efter lovens § 12.

På baggrund af Artikel 29-gruppens fortolkningsbidrag vedrørende forordningens artikel 6, stk. 1, litra f, 2. afsnit, nævnt ovenfor, hvorefter der i hvert fald fremover synes at være mulighed for at fortolke "en opgave i samfundet interesse" bredt, er det mest nærliggende at antage, at faktisk forvaltningsvirksomhed fremover kan rummes inden for forordningens artikel 6, stk. 1, litra e, om *samfundets interesse*.

På tilsvarende vis må offentlige myndigheder, når de behandler personoplysninger som arbejdsgiver, fremover kunne anvende artikel 6, stk. 1, litra e, om "en opgave i samfundet interesse" som behandlingshjemmel, selvom bestemmelsen, med Artikel 29-gruppens ord som nævnt ovenfor, fordrer en streng fortolkning og klar identifikation af den forfulgte offentlige interesse, der berettiger behandlingen. I hvert fald synes Artikel 29-gruppens fortolkningsbidrag om forordning nr. 45/2001, som omtalt umiddelbart ovenfor, at vise, at eksempler som videoovervågning af lokaler af hensyn til sikkerheden, elektronisk overvågning af e-mailtrafik eller personaleevalueringer kan rummes indenfor "en opgave i samfundets interesse". Artikel 29-gruppen synes i den forbindelse at forudsætte, at behandling af personoplysninger som led i myndigheders "forvaltning og drift" skal anses for lovligt – mest nærliggende inden for artikel 6, stk. 1, litra e, om samfundets interesse, hvis undtagelsen i artikel 6, stk. 1, litra f, fortolkes bredt.

3.3.4. Overvejelser

Databeskyttelsesforordningens artikel 6, stk. 1, litra a, b og c, er udtryk for en videreførelse af gældende ret.

Forordningens artikel 6, stk. 1, litra d, ses endvidere ikke at være en ændring i forhold til gældende ret – dog vil bestemmelsen fremover også finde anvendelse i forbindelse med en anden persons vitale interesser, hvilket er en ændring i forhold til gældende ret.

Forordningens artikel 6, stk. 1, litra e, ses overordnet at være i overensstemmelse med gældende ret. Som anført, indeholder databeskyttelsesforordningens artikel 6, stk. 1, litra e, dog ikke en selvstændig hjemmel til, at en dataansvarlig i forbindelse med videregivelse til tredjemand vil kunne tillægge det betydning, om videregivelsen er begrundet i en myndighedsudøvelse, som er blevet pålagt denne tredjemand. Dette ses dog reelt ikke at få nogen indholdsmæssig betydning for behandlingsreglerne, idet det vurderes, at den dataansvarlige i stedet vil kunne bruge *hensynet til samfundets interesse* som selvstændig hjemmel hertil.

Forordningens artikel 6, stk. 1, litra f, 1. afsnit, ses – udover nyskabelsen med det særlige hensyn til børn – ikke at være en ændring i forhold til gældende ret, hvorfor gældende ret efter den 25. maj 2018 vil kunne videreføres.

Forordningens artikel 6, stk. 1, litra f, 2. afsnit, om, at offentlige myndigheder ikke, som led i udførelsen af deres opgaver kan foretage lovlig behandling af hensyn til at forfølge en legitim interesse, er en nyskabelse i forhold til gældende ret. Bestemmelsen vil herefter føre til, at hjemlen til behandling at personoplysninger for offentlige myndigheder, som led i udførelsen af deres opgaver, vil skulle findes i de øvrige behandlingshjemler i forordningens artikel 6, stk. 1 – særligt artikel 6, stk. 1, litra c og e – idet forordningens artikel 6, stk. 1, litra f, 1. afsnit, ikke finder anvendelse. For så vidt angår det ansættelsesretlige område henvises til afsnit 10.4. om ansættelsesforhold, artikel 88.

3.4. Lovlig behandling af ikke-følsomme oplysninger – nationalt råderum, artikel 6, stk. 2-3

3.4.1. Præsentation

Af databeskyttelsesforordningens artikel 6, stk. 2, følger det, hvordan medlemsstaterne kan tilpasse anvendelsen af databeskyttelsesforordningens bestemmelser om behandling med henblik på overholdelse af artikel 6, stk. 1, litra c og e.

Efter artikel 6, stk. 2, overlades medlemsstaterne at fastsætte mere præcist specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling.

I artikel 6, stk. 3, fastsættes det, at grundlaget for behandling i henhold til artikel 6, stk. 1, litra c og e, skal fremgå af EU-retten eller medlemsstaternes nationale ret.

Endvidere følger det af artikel 6, stk. 3, at dette retsgrundlag kan indeholde specifikke bestemmelser med henblik på at tilpasse anvendelsen af bestemmelserne i databeskyttelsesforordningen. I den forbindelse er oplistet en ikke udtømmende liste af eksempler på, hvad de specifikke bestemmelser kan indeholde.

Sammen med præambelbetragtning nr. 10 til databeskyttelsesforordningen fastsætter artikel 6, stk. 2 og 3, således, hvordan medlemsstaterne har mulighed for at præcisere anvendelsen af databeskyttelsesforordningens bestemmelser i forbindelse med de situationer, som vedrører behandling efter forordningens artikel 6, stk. 1, litra c og e, om behandling på baggrund af en retlig forpligtelse eller af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse.

3.4.2. Gældende ret

Det fremgår af artikel 1 i databeskyttelsesdirektivet, at direktivets formål er, at medlemsstaterne i overensstemmelse med dette direktiv (1) sikrer beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger samt, (2) at medlemsstaterne ikke, af grunde, der har forbindelse med den foreskrevne beskyttelse, må indskrænke eller forbyde fri udveksling af personoplysninger mellem medlemsstaterne.

Databeskyttelsesdirektivet beskytter således på den ene side fysiske personers grundlæggende rettigheder og på den anden side den frie udveksling af personoplysninger.

Det fremgår af artikel 5 i databeskyttelsesdirektivet, at medlemsstaterne i henhold til bestemmelserne i kapitel II, vedrørende almindelige betingelser for lovlig behandling af personoplysninger, præciserer, på hvilke betingelser behandling af personoplysninger er lovlig.

Af præambelbetragtning nr. 9 til databeskyttelsesdirektivet fremgår det, at med den ensartede beskyttelse, som vil følge af den indbyrdes tilnærmelse af de nationale lovgivninger, vil medlemsstaterne ikke længere under henvisning til det enkelte menneskes rettigheder og frihedsrettigheder, navnlig retten til privatlivets fred, kunne lægge hindringer i vejen for den frie udveksling af personoplysninger medlemsstaterne imellem.

Det fremgår endvidere af præambelbetragtning nr. 9 til direktivet, at medlemsstaterne vil få en manøvremargen, som erhvervslivet og arbejdsmarkedets parter kan benytte sig af i forbindelse med direktivets gennemførelse; de vil således i deres nationale lovgivning kunne fastsætte de generelle betingelser for lovlig behandling af personoplysninger; medlemsstaterne skal derved tilsigte en forbedring af den beskyttelse, som deres nuværende lovgivning sikrer; inden for rammerne af denne manøvremargen og i overensstemmelse med fællesskabsretten kan der forekomme forskelle i gennemførelsen af direktivet, og dette kan få konsekvenser for udvekslingen af oplysninger såvel inden for den enkelte medlemsstat som på fællesskabsplan.

Det fremgår derudover af præambelbetragtning nr. 22 til databeskyttelsesdirektivet, at medlemsstaterne i deres lovgivning eller i de bestemmelser i øvrigt, der vedtages til gennemførelse af dette direktiv, nærmere fastsætter bestemmelser om, på hvilke generelle betingelser en behandling er lovlig; især artikel 5 giver i forbindelse med artikel 7 og 8 medlemsstaterne mulighed for uafhængigt af de generelle regler at fastsætte særlige betingelser for databehandling på specifikke områder og med hensyn til de særlige kategorier af de oplysninger, der omhandles i artikel 8.

Det fremgår endvidere af præambelbetragtning nr. 30 til databeskyttelsesdirektivet, at en behandling vil være lovlig, hvis behandlingen er begrundet i en persons legitime interesse, medmindre den registreredes interesser, grundlæggende rettigheder og frihedsrettigheder går forud herfor.

Det fremgår endelig af præambelbetragtning nr. 30 til direktivet, at særligt med henblik på at tilgodese de involverede interesser ligeligt og samtidig sikre en effektiv konkurrence kan medlemsstaterne fastsætte nærmere bestemmelser om, på hvilke betingelser anvendelse og videregivelse af personoplysninger til tredjemand kan finde sted i forbindelse med legitime aktiviteter udøvet af virksomheder og andre organer som led i den daglige drift. De kan ligeledes fastsætte nærmere bestemmelser om, på hvilke betingelser videregivelse af personoplysninger til tredjemand kan finde sted i forbindelse med markedsføring eller markedsundersøgelser, der udføres af velgørende organisationer eller andre sammenslutninger eller stiftelser, f.eks. af politisk karakter, under overholdelse af bestemmelser, som har til formål at give den registrerede mulighed for uden begrundelse og udgifter at gøre indsigelse mod, at sådanne oplysninger behandles.

I sag C-101/01, Lindqvist, dom af 6. november 2003, havde en person oprettet hjemmesider på internettet indeholdende oplysninger om hendes kolleger for at gøre det let for medlemmer af en menighed at forberede konfirmation. Hjemmesiderne indeholdt oplysninger om bl.a. 18 kolleger, herunder med navn og oplysning om kollegernes arbejdsopgaver og

fritidsvaner. I flere tilfælde var også deres telefonnummer og familieforhold anført. Endelig var der om en af kollegerne oplyst, at hun havde beskadiget foden og var delvist sygemeldt.

EU-Domstolen anførte i præmis 96, at harmoniseringen af de nationale lovgivninger ikke er begrænset til en minimumsharmonisering, men fører til en harmonisering, der i princippet er fuldstændig. EU-Domstolen anførte endvidere, at det er i dette perspektiv, at databeskyttelsesdirektivet tilsigter at sikre den frie udveksling af personoplysninger, idet der sikres en høj beskyttelse af de personers rettigheder og interesser, som oplysningerne vedrører.

EU-Domstolen udtalte i præmis 97, at databeskyttelsesdirektivet indrømmer medlemsstaterne et råderum på visse områder, og de bemyndiges til at opretholde eller indføre særlige ordninger med henblik på specifikke tilfælde, hvilket mange af dets bestemmelser vidner om. Disse muligheder skal imidlertid anvendes på den måde, som er fastsat i databeskyttelsesdirektivet, og i overensstemmelse med dets formål, som består i at opretholde en ligevægt mellem den frie udveksling af personoplysninger og beskyttelsen af privatlivet.

EU-Domstolen udtalte endelig i præmis 99, at de foranstaltninger, som medlemsstaterne træffer med henblik på at sikre beskyttelsen af personoplysninger, skal være forenelige med såvel bestemmelserne i databeskyttelsesdirektivet som med dets formål, som består i at opretholde en ligevægt mellem den frie udveksling af personoplysninger og beskyttelsen af privatlivet.

I sag C-468/10, Asociación National de Establecimientos Finansieros de Crédito (ASNEF), dom af 24. november 2011, blev EU-Domstolen forelagt et præjudicielt spørgsmål af en spansk domstol om, hvorvidt artikel 7, litra f, i databeskyttelsesdirektivet skal fortolkes således, at den er til hinder for en national lovgivning, som, i tilfælde af at den registrerede ikke har givet sit samtykke, og for at muliggøre behandlingen af den pågældendes personoplysninger, som er nødvendig for, at den dataansvarlige eller de tredjemænd, til hvem de videregives, kan forfølge en legitim interesse, ud over at den registreredes grundlæggende rettigheder og frihedsrettigheder ikke krænkes, kræver, at oplysningerne er opført i offentligt tilgængelige kilder.

Den pågældende spanske lov opstillede således en yderligere betingelse i artikel 7, litra f, for gyldig behandling. Udover kravet i bestemmelsen om opfyldelse af en legitim interesse, krævede den spanske lov således, at oplysningerne fremgik af et offentligt tilgængeligt register.

EU-Domstolen fastslog, at det følger af databeskyttelsesdirektivets formål, som består i at sikre et ensartet beskyttelsesniveau i alle medlemsstaterne, at direktivets artikel 7 fastsætter en udtømmende og fuldstændig liste over de tilfælde, hvor behandling af personoplysninger kan anses for at være lovlig. Domstolen anførte herefter, at medlemsstaterne derfor hverken kan tilføje nye principper vedrørende grundlaget for behandling af oplysninger i artikel 7 eller fastsætte supplerende krav, som ændrer rækkevidden af et af de seks principper, der er fastsat i denne artikel.

EU-Domstolen udtalte i præmis 35, at databeskyttelsesdirektivet indeholder bestemmelser, der er kendetegnet ved en vis fleksibilitet, og i mange tilfælde overlader medlemsstaterne at fastlægge detaljerne eller at vælge mellem muligheder. Domstolen anførte, at det således er vigtigt at sondre mellem nationale foranstaltninger, som fastsætter *supplerende* krav, der ændrer rækkevidden af et i artikel 7 i databeskyttelsesdirektivet fastsat princip, på den ene side, og nationale foranstaltninger, som blot *præciserer* et af disse principper, på den anden side. Den første type nationale foranstaltninger er forbudt. Det er kun i forbindelse med den anden type nationale foranstaltninger, at medlemsstaterne i henhold til artikel 5 i databeskyttelsesdirektivet råder over et skøn.

Endelig udtalte Domstolen i præmis 36, at medlemsstaterne heller ikke i medfør af artikel 5 i databeskyttelsesdirektivet kan indføre andre principper vedrørende grundlaget for behandling af personoplysninger end dem, der er opregnet i dette direktivs artikel 7, eller ved supplerende krav ændre rækkevidden af de seks principper, der er fastsat i databeskyttelsesdirektivets artikel 7.

I sag C-683/13, Pharmacontinente-Saúde e Higiene SA m.fl. mod Autoridade Para As Condições do Trabalho (ACT), af 19. juni 2014, udtalte EU-Domstolen, at databeskyttelsesdirektivets artikel 7, litra c og e, skal fortolkes således, at det ikke er til hinder for en national lovgivning, som pålægger arbejdsgiveren en forpligtelse til at stille et arbejdstidsregister til rådighed for den kompetente nationale tilsynsmyndighed på en måde, der muliggør umiddelbar aflæsning, for så vidt som denne forpligtelse er nødvendig med henblik på denne myndigheds gennemførelse af sine tilsynsopgaver med forvaltningen af lovgivningen på området for arbejdsvilkår, bl.a. for så vidt angår arbejdstid.

I sag C-582/14, Patrick Breyer, dom af 19. oktober 2016, blev EU-Domstolen forelagt et præjudicielt spørgsmål af en tysk domstol om, hvorvidt artikel 7, litra f, i databeskyttelsesdirektivet skal fortolkes således, at den er til hinder for en lovgivning i en medlemsstat, hvorefter en udbyder af online-medietjenester kun må indsamle og anvende personoplysninger om en bruger af disse tjenester uden samtykke fra denne, i det omfang denne indsamling og denne anvendelse er nødvendig for at give adgang til og afregne for den kon-

krete anvendelse af de nævnte tjenester foretaget af denne bruger, uden at formålet om at sikre de samme tjenesters generelle funktionsdygtighed kan begrunde anvendelsen af de nævnte oplysninger efter en søgning på disse tjenester.

EU-Domstolen anførte i præmis 62, at interesseafvejningsreglen i direktivets artikel 7, litra f, er til hinder for, at en medlemsstat kategorisk og generelt udelukker muligheden for behandling af visse kategorier af personoplysninger uden at tillade en afvejning af de i en konkret sag foreliggende modstående rettigheder og interesser. En medlemsstat kan således ikke for disse kategorier definitivt foreskrive resultatet af afvejningen af de modstående rettigheder og interesser uden at tillade et anderledes resultat som følge af særlige omstændigheder i det konkrete tilfælde.

EU-Domstolen udtalte endvidere i præmis 64, at artikel 7, litra f, i direktivet skal fortolkes således, at den er til hinder for en lovgivning i en medlemsstat, hvorefter en udbyder af online-medietjenester kun må indsamle og anvende personoplysninger om en bruger af disse tjenester uden samtykke fra denne, i det omfang denne indsamling og denne anvendelse er nødvendig for at give adgang til og afregne for den konkrete anvendelse af de nævnte tjenester foretaget af denne bruger, uden at formålet om at sikre de samme tjenesters generelle funktionsdygtighed kan begrunde anvendelsen af de nævnte oplysninger efter en søgning på disse tjenester.

I denne dom var der således tale om, at den tyske lovgivning i en særregel begrænsede rækkevidden af bestemmelsen i direktivets artikel 7, litra f, til, at det kun er nogle bestemte legitime formål, som vil kunne begrunde en behandling. Dette vurderede EU-Domstolen som værende i strid med direktivet.

Dommen ses at være på linje med afgørelsen i ASNEF-dommen, der også vedrørte interesseafvejningsreglen i direktivets artikel 7, litra f, hvoraf det som anført netop fremgik, at medlemsstaterne ikke ved supplerende krav kan ændre rækkevidden af de seks principper, der er fastsat i databeskyttelsesdirektivets artikel 7. National lovgivning må dog som nævnt gerne indeholde regler, der blot præciserer et af disse principper.

Det følger af gældende ret, særligt på baggrund af praksis fra EU-Domstolen, at databeskyttelsesdirektivet skal fortolkes i overensstemmelse med direktivets formål, som fremgår af direktivets artikel 1. Ved vurderingen af det nationale råderum skal der derfor både tages hensyn til på den ene side fysiske personer og på den anden side den frie udveksling af personoplysninger mellem medlemsstaterne. Medlemsstaterne kan hverken tilføje nye principper vedrørende grundlaget for behandling af oplysninger i databeskyttelsesdirektivets artikel 7 eller fastsætte supplerende krav, som ændrer rækkevidden af et af de seks

principper. Men det overlades til medlemsstaterne at præcisere principperne i databeskyttelsesdirektivets artikel 7, herunder også at fastslå, hvad der er en retlig forpligtelse eller offentlig myndighedsudøvelse efter artikel 7, litra c og e.

Efter gældende ret er det inden for det nationale råderum, som databeskyttelsesdirektivet fastlægger, således muligt at vedtage særlovgivning.

I Danmark er der på den baggrund vedtaget en betydelig mængde særlovgivning og særlige bestemmelser inden for det persondataretlige område bl.a. i lov om det centrale personregister, lov om finansiel virksomhed, skattekontrolloven, lov om retssikkerhed og administration på det sociale område, lov om Udbetaling Danmark.

3.4.3. Databeskyttelsesforordningen

Det fremgår af databeskyttelsesforordningens artikel 1, stk. 2, at forordningen beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger.

Det fremgår endvidere af databeskyttelsesforordningens artikel 1, stk. 3, at den frie udveksling af personoplysninger i EU hverken må indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

I den forbindelse fremgår det af præambelbetragtning nr. 13, at for at sikre et ensartet beskyttelsesniveau for fysiske personer i hele EU og for at hindre, at forskelle hæmmer den frie udveksling af personoplysninger på det indre marked, er der behov for en forordning for at skabe retssikkerhed og gennemsigtighed for erhvervsdrivende, herunder mikrovirksomheder og små og mellemstore virksomheder, at give fysiske personer i alle medlemsstaterne det samme niveau af rettigheder, som kan håndhæves, og forpligtelser og ansvar for dataansvarlige og databehandlere og at sikre konsekvent tilsyn med behandling af personoplysninger og tilsvarende sanktioner i alle medlemsstaterne samt effektivt samarbejde mellem tilsynsmyndighederne i de forskellige medlemsstater.

Det fremgår endvidere af præambelbetragtning nr. 13, at et velfungerende indre marked kræver, at den frie udveksling af personoplysninger i EU hverken indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

I Lindqvist-dommen, der er omtalt i ovenstående afsnit, fastslog EU-Domstolen som nævnt, at databeskyttelsesdirektivet førte til en harmonisering, der i princippet er fuldstæn-

dig. Databeskyttelsesdirektivets mulighed for et nationalt råderum vil derfor have betydning i forhold til vurderingen af det nationale råderum i databeskyttelsesforordningen.

I præambelbetragtningerne til databeskyttelsesforordningen refereres der ikke til praksis fra EU-Domstolen. Det må dog kunne lægges til grund, at praksis fra EU-Domstolen, som vedrører bestemmelser fra databeskyttelsesdirektivet, der også er medtaget i forordningen, fortsat vil kunne anvendes som retningsgivende.

EU-Domstolen udtalte i Lindqvist-dommen, at medlemsstaterne indrømmes et råderum på visse områder, og de bemyndiges til at opretholde eller indføre særlige ordninger med henblik på specifikke tilfælde. Domstolen udtalte endvidere, at disse muligheder imidlertid skal anvendes på den måde, som er fastsat i databeskyttelsesdirektivet og i overensstemmelse med dets formål, som består i at opretholde en ligevægt mellem den frie udveksling af personoplysninger og beskyttelsen af privatlivet.

Ordlyden i databeskyttelsesforordningens artikel 1, stk. 2 og 3, ses næsten at være identisk med ordlyden i databeskyttelsesdirektivets artikel 1. Ud fra en ordlydsfortolkning af databeskyttelsesdirektivets og databeskyttelsesforordningens formålsbestemmelser ses disse således at have et identisk formål – netop både beskyttelsen af personoplysninger samt den frie udveksling af personoplysninger i EU. På baggrund af Lindqvist-dommen sammenholdt med, at formålet i databeskyttelsesforordningen fremgår af artikel 1, vil medlemsstaternes manøvremargen i relation til databeskyttelsesforordningen fortsat skulle fortolkes i overensstemmelse med formålet i forordningen.

3.4.3.1. Databeskyttelsesforordningens artikel 6, stk. 2

Det fremgår af databeskyttelsesforordningens artikel 6, stk. 2, at medlemsstaterne *kan* opretholde eller indføre mere specifikke bestemmelser for at tilpasse anvendelsen af denne forordnings bestemmelser om behandling med henblik på overholdelse af stk. 1, litra c og e, ved at fastsætte mere præcist specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling, *herunder* for andre specifikke databehandlingssituationer som omhandlet i kapitel IX (artikel 85-91).

Det fremgår endvidere af præambelbetragtning nr. 10, at i forbindelse med behandling af personoplysninger for at overholde en retlig forpligtelse eller for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, bør medlemsstaterne kunne opretholde eller indføre nationale bestemmelser for yderligere at præcisere anvendelsen af denne forordnings bestemmelser. Det fremgår af samme præambelbetragtning, at sammen med generel og horisontal lovgivning om databeskyttelse til gennemførelse af databeskyttelsesdirektivet har med-

lemsstaterne flere sektorspecifikke love på områder, hvor der er behov for mere specifikke bestemmelser.

Det fremgår endvidere af præambelbetragtning nr. 10, at denne forordning også indeholder en manøvremargen, så medlemsstaterne kan præcisere reglerne heri, herunder for behandling af særlige kategorier af personoplysninger omfattet af artikel 9.

Det fremgår endelig af præambelbetragtning nr. 10, at forordningen således ikke udelukker, at medlemsstaternes nationale ret fastlægger omstændighederne i forbindelse med specifikke databehandlingssituationer, herunder mere præcis fastlæggelse af de forhold, hvorunder behandling af personoplysninger er lovlig.

I denne præambelbetragtning nævnes som anført, at medlemsstaterne kan opretholde eller indføre nationale bestemmelser for yderligere at *præcisere* anvendelsen af databeskyttelsesforordningens bestemmelser. Denne betragtning ses umiddelbart at være i tråd med EU-Domstolens dom i ASNEF-sagen og i Patrick Breyer-sagen, hvor Domstolen netop anfører, at der imidlertid skal tages hensyn til det skøn, som medlemsstaterne har i forbindelse med gennemførelsen af databeskyttelsesdirektivet til i national ret at *præcisere* de almindelige betingelser for lovligheden af behandlingen af personoplysninger.

ASNEF-dommen og Patrick Breyer-dommen ændrer ikke ved, at medlemsstaternes i medfør af forordningens artikel 6, stk. 1, litra c og e, kan – "præcisere" – disse bestemmelser ved nærmere at fastslå, hvad der er en retlig forpligtelse og offentlig myndighedsudøvelse.

Det er således netop op til medlemsstaterne i deres nationale ret samt EU-lovgiver i EU-retten at fastsætte, hvad der er en retlig forpligtelse, og herunder også hvad der er offentlig myndighedsudøvelse, og derfor hvornår nærmere behandling kan ske efter disse behandlingshjemler. Medlemslandene har altså mulighed for at fastsætte nærmere regler herom.

Dette fremhæves også særligt i præambelbetragtning nr. 10, hvoraf det fremgår, at forordningen ikke udelukker, at medlemsstaternes nationale ret fastlægger omstændighederne i forbindelse med specifikke databehandlingssituationer, herunder mere præcis fastlæggelse af de forhold, hvorunder behandling af personoplysninger er lovlig.

Efter ordlyden af denne betragtning er det netop op til medlemslandene at præcisere, hvornår en behandling er lovlig, og ASNEF-dommen og Patrick Breyer-dommen ses ikke at begrænse medlemsstaternes mulighed for at fastslå, hvad der er en retlig forpligtelse eller offentlig myndighedsudøvelse, da der derved med dommens sprogbrug blot er tale om en præcisering.

Det fremgår af præambelbetragtning nr. 45, at forordningen ikke indebærer, at der kræves en specifik lov til hver enkelt behandling. Det kan være tilstrækkeligt med en lov som grundlag for adskillige databehandlingsaktiviteter, som baseres på en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse.

Det må antages, at når EU-lovgiver i præambelbetragtning nr. 10 har anført, at medlemsstaterne bør kunne *opretholde* eller indføre nationale bestemmelser for yderligere at præcisere anvendelsen af denne forordnings bestemmelser, vil det være sådan, at medlemsstaternes nuværende lovgivning, som ses at være i overensstemmelse med gældende ret, også efter forordningens ikrafttrædelse som udgangspunkt vil kunne opretholdes.

Som anført i afsnit 3.3. om lovlig behandling af ikke-følsomme oplysninger, artikel 6, stk. 1, konkluderes det, at databeskyttelsesforordningens artikel 6, stk. 1, litra c og e, er en videreførelse af gældende ret. Heraf kan det således sammenholdt med præambelbetragtning nr. 10 antages, at medlemsstaterne også efter den 25. maj 2018 vil kunne opretholde lovgivning, som er inden for rammerne af litra c og e om en retlig forpligtelse samt en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse.

Betingelserne for hvornår der efter forordningens artikel 6, stk. 1, litra c og e, foreligger en retlig forpligtelse samt en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse behandles nærmere i afsnit 3.3. om lovlig behandling af ikke-følsomme oplysninger, artikel 6, stk. 1.

Databeskyttelsesforordningens generelle formål, ordlyden i forordningens artikel 6, stk. 2, samt præambelbetragtning nr. 10 indikerer ikke, at det har været hensigten, at der med databeskyttelsesforordningen er tiltænkt et andet rum – end efter databeskyttelsesdirektivet – for at fastsætte mere specifikke nationale krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling med henblik på overholdelse af artikel 6, stk. 1, litra c og e, hvorfor det nationale råderum på dette område er i overensstemmelse med databeskyttelsesdirektivet og en videreførelse af gældende ret.

Der er dog den forskel i forhold til gældende ret, at det eksplicit i databeskyttelsesforordningens artikel 6, stk. 2, nævnes, at muligheden for, at medlemsstaterne kan opretholde eller indføre mere specifikke bestemmelser, er med henblik på at overholde artikel 6, stk. 1, litra c og e.

Der er således ud fra ordlyden i artikel 6, stk. 2, i princippet, tale om en indskrænkning i forhold til gældende ret, hvorefter medlemsstaterne blev overladt mulighed for at præcisere

betingelserne for behandling af personoplysninger i henhold til bestemmelserne i kapitel II (det vil sige bl.a. databeskyttelsesdirektivets artikel 6, 7 og 8), jf. databeskyttelsesdirektivets artikel 5.

I forhold til behandlingen efter artikel 6, stk. 1, litra a, b og d, vil denne indskrænkning i forhold til databeskyttelsesdirektivet – særligt i lyset af ASNEF-dommen – ikke have den store praktiske betydning. I forhold til artikel 6, stk. 1, litra a, indeholder databeskyttelsesforordningen mange præciserende regler om samtykkets karakter, se særligt artikel 4, nr. 11, og artikel 7, hvorfor det i praksis ikke ses at være relevant, hvis medlemsstaterne overlades en yderligere mulighed for at fastsætte mere præcist specifikke krav hertil.

Endvidere vil det ikke være relevant for en medlemsstat at fastsætte yderligere regler for artikel 6, stk. 1, litra b og d, idet disse bestemmelser har et smallere og *klarere* anvendelsesområde, end det er tilfældet med artikel 6, stk. 1, litra c og e, som efterlader et forholdsvist stort rum både for fortolkning og yderligere lovgivning.

På baggrund af ordlyden i artikel 6, stk. 2, sammenholdt med præambelbetragtning nr. 10 ses medlemsstaterne heller ikke at blive overladt muligheden for at tilpasse anvendelsen af databeskyttelsesforordningens bestemmelser om behandling for så vidt angår behandling, som er nødvendig af hensyn til en legitim interesse efter databeskyttelsesforordningens artikel 6, stk. 1, litra f, hvilket stemmer fint overens med ASNEF-dommen og Patrick Breyer-dommen.

Det må herefter konkluderes, at da det eksplicit anføres, at artikel 6, stk. 2, kun vedrører artikel 6, stk. 1, litra c og e, og sammenholdt med præambelbetragtning nr. 10, vil medlemsstaterne ikke være overladt en mulighed for mere præcist at fastsætte specifikke krav til behandling og andre foranstaltninger for så vidt angår artikel 6, stk. 1, litra a, b, d og f. Det samme gælder vedrørende databeskyttelsesforordningens artikel 6, stk. 3, som omtales umiddelbart nedenfor.

ASNEF-dommen og Patrick Breyer-dommen, som er omtalt i ovenstående afsnit, vedrørte netop behandling efter en bestemmelse, som svarer til databeskyttelsesforordningens artikel 6, stk. 1, litra f, hvorefter der således efter databeskyttelsesforordningen nu ikke længere ses at være samme mulighed for at præcisere anvendelsen i forbindelse med litra f. Dette vil dog formentlig ikke få den store praktiske betydning, idet anvendelsen af artikel 6, stk. 1, litra f, i forvejen begrænses i databeskyttelsesforordningen, idet bestemmelsen ikke længere finder anvendelse for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

Når offentlige myndigheder behandler personoplysninger med hjemmel i forordningens artikel 6, stk. 1, litra a, må samtykket – i overensstemmelse med retningen i ASNEF-dommen og Patrick Breyer-dommen – skulle være i overensstemmelse med samtykket i forordningen, som nærmere beskrives i artikel 4, nr. 11, og artikel 7.

Således må en bestemmelse som § 11 a i lov om retssikkerhed og administration på det sociale område[178], hvorefter myndigheden efter forudgående samtykke fra den, der søger om eller får hjælp, kan forlange, at andre offentlige myndigheder mv. giver oplysninger om den pågældende, der er nødvendige for at behandle sagen, skulle forstås i overensstemmelse med forordningens samtykkeregler i artikel 6, stk. 1, litra a, og artikel 9, stk. 2, litra a – og i øvrigt artikel 7.

En sådan national lovgivning kan – som en slags "dobbelt-hjemmel" – samtidigt vedtages inden for rammerne af artikel 6, stk. 1, litra e (for ikke-følsomme oplysningers vedkommende).

Omvendt må medlemsstaterne på baggrund af (alene) artikel 6, stk. 1, litra e, kunne vedtage en lovgivning, der kræver behandling af personoplysninger, og hvor der – som en slags garanti for den registrerede – kræves et *stiltiende* samtykke.

Et sådan eksempel findes i arbejdsskadesikringslovens § 37 a, hvorefter der i arbejdsskadesager kan indhentes samtykke ved, at tilskadekomne eller efterladte i den skriftlige bekræftelse af, at en anmeldelse er modtaget, bliver gjort opmærksom på, hvilke typer af oplysninger det kan blive nødvendigt at indhente, og får en frist til eventuelt at gøre indsigelse imod dette.

Forordningen anerkender ikke et stiltiende samtykke som gyldigt behandlingsgrundlag, og samtykkekravet i arbejdsskadesikringslovens § 37 a lever således ikke op til forordningens krav til gyldigt samtykke, jf. nærmere definitionen i artikel 4, nr. 11.

Et sådant krav om stiltiende samtykke må dog kunne vedtages i en national lovgivning med henvisning til alene artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2-3, om bl.a. behandling og lovgivning i samfundets interesse. Det stiltiende samtykke skal her ses som et nationalt krav – en garanti – der sikrer overholdelse af krav til proportionalitet mv. efter forordningens artikel 5.[179]

[178] Bekendtgørelse af lov om retssikkerhed og administration på det sociale område, jf. lovbekendtgørelse nr. 1052 af 8. september 2015.
[179] Det bemærkes, at behandling af personoplysninger efter arbejdsskadesikringslovens § 37 a ofte vil indebære behandling af følsomme oplysninger (helbredsoplysninger) omfattet af artikel 9. Eksemplet anvendes

Konsekvensen heraf er også, at forordningens artikel 7 om betingelser for samtykke ikke finder anvendelse på en national bestemmelse som arbejdsskadesikringslovens § 37 a, der alene har sit hjemmelsmæssige udgangspunkt i – for så vidt angår ikke-følsomme oplysninger – forordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2-3, og ikke stk. 1, litra a, da artikel 7 alene finder anvendelse, når der er tale om et samtykke i forordningens forstand.

Der kan i den forbindelse også henvises til, at forordningens præambelbetragtning nr. 43, hvorefter samtykke ikke bør udgøre et gyldigt retsgrundlag for behandlingen, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige, navnlig hvis den dataansvarlige er en offentlig myndighed, må antages at indeholde en intention om, at offentlige myndigheders brug af samtykke i forordningens forstand skal begrænses.

Spørgsmålet rejser sig i forlængelse heraf, om medlemsstaterne kan vedtage lovgivning efter forordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2-3, hvorefter behandling af oplysninger *alene* kan ske, hvis bestemte betingelser er opfyldt – underforstået, at andre behandlingshjemler f.eks. i artikel 6, stk. 1, f.eks. behandling efter litra d af hensyn til den registreredes eller en anden fysisk persons vitale interesser, ikke kan anvendes som behandlingsgrundlag.

En sådan kategorisk lovbestemmelse kunne umiddelbart være vanskelig forenelig med ASNEF-dommen og Breyer-dommen, omtalt ovenfor, hvorefter EU-Domstolen om databeskyttelsesdirektivets artikel 7 udtalte, at direktivbestemmelsen fastsætter en udtømmende og fuldstændig liste over de tilfælde, hvor en behandling af personoplysninger kan anses for at være lovlig, og at medlemsstaterne hverken kan tilføje nye principper vedrørende grundlaget for behandling af personoplysninger i den nævnte artikel eller fastsætte *supplerende* krav, som ændrer rækkevidden af et af de seks principper, der er fastsat i direktivets artikel 7 litra a-f, jf. præmis 57 i Breyer-dommen.

Medlemsstaterne må dog i henhold til direktivets artikel 5 præcisere de betingelser, hvorunder behandling af personoplysninger er lovlig, men alene hvis præciseringen sikrer en opretholdelse af en ligevægt mellem den frie udveksling af personoplysninger og beskyttelsen af privatlivet. Medlemsstaterne kan dog ikke i den forbindelse indføre andre principper vedrørende grundlaget for behandling af personoplysninger end dem, der er opregnet i dets artikel 7, eller ved supplerende krav ændre rækkevidden af de seks principper, der er fastsat i nævnte artikel 7, jf. præmis 58 i Breyer-dommen.

---

dog her til at illustrere rækkevidden af det nationale råderum i artikel 6, stk. 2-3, jf. artikel 6, stk. 1, litra e. Det samme vil også kunne gøre sig gældende ved behandling af personoplysninger efter § 11 a i lov om retssikkerhed og administration på det sociale område og forvaltningslovens § 29, der omtales senere.

Det ligger dog fast, at medlemsstaterne i en national lov kan *præcisere*, hvad der på et specifikt område skal ligge i "samfundets interesse" og/eller "offentlig myndighedsudøvelse" – i overensstemmelse med forordningens præambelbetragtning 10 og artikel 6, stk. 2-3 samt ASNEF-dommen og Breyer-dommen.

Et sådant eksempel på en national behandlingshjemmel, hvorefter behandling af oplysninger *alene* kan ske, hvis bestemte betingelser er opfyldt, findes i forvaltningslovens § 29, hvorefter der i ansøgningssager vedrørende ansøgerens rent private forhold alene må indhentes oplysninger fra andre dele af forvaltningen eller fra en anden forvaltningsmyndighed, hvis ansøgeren har givet samtykke hertil, andet følger af lov eller bestemmelser fastsat i henhold til lov eller særlige hensyn til ansøgeren eller tredjemand klart overstiger ansøgerens interesse i, at oplysningen ikke indhentes.

Bestemmelsen i forvaltningslovens § 29 må antages at ligge inden for rammerne for national særlovgivning i forordningens artikel 6, stk. 2, hvorefter de skal vedrøre "specifikke krav til behandling" eller "specifikke databehandlingssituationer".

Grænsen i artikel 6, stk. 2, om bl.a. "specifikke krav" må i hvert fald betyde, at nationale særregler om, hvornår behandling er lovlig, ikke kan vedrøre alle behandlingssituationer på mange områder (såsom eksempelvis persondatalovens §§ 6-7). Særreglen skal således på en eller anden måde begrænse sig – vertikalt *eller* horisontalt – til et bestemt område eller en bestemt behandlingssituation.

Forvaltningslovens § 29 begrænser sig til ansøgningssager og falder således inden for artikel 6, stk. 2's rammer. Selvom bestemmelsen er bred horisontalt set, fordi den vedrører alle ansøgningssager hos offentlige myndigheder, er reglen alligevel meget begrænset i sit anvendelsesområde, da den netop alene vedrører ansøgningssager og ikke andre sager.

Bestemmelsen må derfor antages at være tilstrækkelig afgrænset – og dermed vedrøre en "specifik databehandlingssituation" – til, at den ligger inden for artikel 6, stk. 2's rammer for national særlovgivning. Det bemærkes i den forbindelse, at artikel 6, stk. 2, henviser til databeskyttelsesforordningens kapitel 9, der eksempelvis indeholder en *vertikal* regel om ansættelsesforhold, jf. artikel 88, og en *horisontal* regel om ytrings- og informationsfriheden, jf. artikel 85.

Forvaltningslovens § 29 fastsætter således på et bestemt område, nemlig i ansøgningssager, betingelserne for, hvornår behandling må ske. Fra den private sektor kan nævnes betalingstjenestelovens § 85, der i stk. 3-5 udtømmende regulerer til hvilke formål, der kan ske be-

handling af oplysninger om, hvor betalingsinstrumenter har været anvendt, og hvad der er købt.[180]

De andre behandlingsgrundlag i forordningens artikel 6, stk. 1, må dog efter ASNEF-dommen og Breyer-dommen antages i princippet stadig at kunne anvendes som behandlingshjemmelsgrundlag i et sådant tilfælde, hvor det nationalt er reguleret, hvornår en behandling af personoplysninger på et specifikt område skal anses for at være lovlig.

Det forekommer i den forbindelse da også naturligt, at man "altid" kan behandle personoplysninger i nødvendigt omfang af hensyn til den registreredes eller en anden fysisk persons *vitale interesser*, jf. artikel 6, stk. 1, litra d, (som i øvrigt nok i vidt omfang er sammenfaldende med værdispringsreglen i forvaltningslovens § 29, stk. 2, nr. 3) ved siden af den pågældende nationale lovgivning.

I praksis må det dog trods alt have begrænset betydning, at de andre behandlingshjemler kan anvendes ved siden af en i princippet udtømmende national lovgivning om behandling. Dette også i lyset af, at interesseafvejningsreglen i artikel 6, stk. 1, litra f, ikke gælder for behandling, som *offentlige myndigheder* foretager som led i udførelsen af deres opgaver.

Selvom interesseafvejningsreglen i artikel 6, stk. 1, litra f, således i princippet finder anvendelse som behandlingsgrundlag ved siden af national lovgivning – vedtaget i overensstemmelse med forordningens artikel 6, stk. 2-3 – der retter sig mod *private*, vil stk. 1, litra f, nok have begrænset betydning selv i en sådan situation.

Der kan i den forbindelse henvises til Artikel 29-gruppens udtalelse 6/2014 om den dataansvarliges *legitime interesser* som omhandlet i artikel 7 i databeskyttelsesdirektivet.[181] Udtalelsen er skrevet bl.a. i forlængelse af ASNEF-dommen, og heraf fremgår, at de første fem grundlag i artikel 7 opstiller den registreredes samtykke, et kontraktforhold, en retlig forpligtelse eller en anden specifikt anført begrundelse som grundlag for lovlighed. Herudover udtaler Artikel 29-gruppen, at når databehandlingen er baseret på et af disse fem grundlag, betragtes den på forhånd som lovlig og skal derfor kun overholde andre gældende lovbestemmelser. Det antages med andre ord, ifølge Artikel 29-gruppen, at der er balance mellem de forskellige berørte rettigheder og interesser – herunder den dataansvarliges og den registreredes – naturligvis under forudsætning af, at alle andre bestemmelser i databeskyttelseslovgivningen overholdes. Artikel 7, litra f, kræver derimod en *specifik* test for tilfæl-

[180] Bekendtgørelse af lov om betalingstjenester og elektroniske penge, jf. lovbekendtgørelse nr. 613 af 24. april 2015 med senere ændringer.
[181] Artikel 29-gruppens udtalelse nr. 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF (WP 217).

de, der ikke passer ind i de scenarier, der er anført i litra a til e. Det sikrer, ifølge Artikel 29-gruppen at databehandling uden for disse scenarier skal opfylde kravene i en afvejningstest, der tager behørigt hensyn til den registreredes interesser og grundlæggende rettigheder.

Det fremgår af ovenstående, at hjemmelsgrundlagene i direktivets artikel 7, litra a-e, er udtryk for en afbalancering af de forskellige berørte rettigheder og interesser, og at det er uden for disse hjemmelsgrundlag, at man som dataansvarlig skal opfylde den specifikke test i litra f, hvis behandling skal anses for lovlig.

I tilknytning hertil behandler udtalelsen fra Artikel 29-gruppen begrebet "legitim interesse" i artikel 7, litra f, i databeskyttelsesdirektivet. Det fremgår herom på side 27 i udtalelsen, at kravet til, at en interesse er "legitim" – og dermed inden for rammerne af artikel 7, litra f – er, at den er lovlig at forfølge, dvs. "i overensstemmelse med gældende EU-lovgivning og national lovgivning".

Som uddybning hertil fremgår det af udtalelsens side 26, at "[e]n interesse kan … betragtes som legitim, når den dataansvarlige kan forfølge den på en måde, som er i overensstemmelse med databeskyttelseslovgivningen og den øvrige lovgivning. En legitim interesse *skal* med andre ord være acceptabel i henhold til lovgivningen." (fremhævet her) Det fremgår i den forbindelse, at begrebet "lovgivning" her anvendes i dets bredeste betydning og omfatter f.eks. lovgivning om ansættelse, kontrakter og forbrugerbeskyttelse.

På den baggrund er det vanskeligt at forestille sig, at en privat dataansvarlig, f.eks. et forsikringsselskab, lovligt kan anvende interesseafvejningsreglen i artikel 6, stk. 1, litra f, i en situation, hvor en medlemsstat – i overensstemmelse med artikel 6, stk. 2-3, jf. artikel 6, stk. 1, litra e – har vedtaget en lovgivning for et specifikt område, f.eks. for hvornår forsikringsselskaber må behandle oplysninger i en given situation, hvis det pågældende nationale lovgrundlag ikke åbner mulighed for behandling i andre situationer.

Endelig må det antages, at forordningens artikel 6, stk. 1, litra e, ikke kan anvendes som behandlingshjemmel, f.eks. af en kommune, hvis behandlingen ville være i strid med en national lovgivning om behandling, som en medlemsstat har vedtaget i overensstemmelse med råderummet i artikel 6, stk. 2-3.

Selvom artikel 6, stk. 1, litra e, som tidligere nævnt er direkte anvendelig som behandlingshjemmel – i det omfang en dataansvarlig udfører en opgave i samfundets interesse eller som led i offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt – kan den direkte anvendelighed således ikke udstrækkes til behandling, der er i strid med en

national lovgivning, der er vedtaget i overensstemmelse med råderummet i forordningens artikel 6, stk. 2-3. Det ville i en sådan situation da også være vanskeligt at hævde, at behandlingen foregik i "samfundets interesse" eller var et led i "offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt".

3.4.3.2. Databeskyttelsesforordningens artikel 6, stk. 3

Det følger af databeskyttelsesforordningens artikel 6, stk. 3, der synes at fastsætte nærmere betingelser for at anvende artikel 6, stk. 2, at grundlaget for behandling i henhold til stk. 1, litra c og e, skal fremgå af EU-retten eller af medlemsstaternes nationale ret, som den dataansvarlige er underlagt.

Databeskyttelsesforordningens artikel 6, stk. 3, skal ses i forlængelse af artikel 6, stk. 2. Artikel 6, stk. 3, er således en uddybning af, hvordan de bestemmelser, som indføres efter artikel 6, stk. 2, hvorefter medlemsstaterne *kan* opretholde eller indføre specifikke regler, nærmere vil skulle udformes.

Selvom det fremgår af artikel 6, stk. 3, 1. punktum, at "grundlaget for behandling i henhold til stk. 1, litra c og e, *skal* fremgå af EU-retten eller medlemsstaternes nationale ret", vurderes ordet "skal" således ikke at få den selvstændige betydning, at f.eks. artikel 6, stk. 1, litra e, ikke vil kunne anvendes som direkte behandlingshjemmel – så længe den dataansvarlige udfører en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Det bemærkes i den forbindelse, at det – i lyset af, at der er tale om en forordning som retsgrundlag – må have en klar formodning for sig, at behandlingsgrundlagene i artikel 6, stk. 1, vil kunne anvendes direkte som behandlingsgrundlag, medmindre noget andet udtrykkeligt fremgår af bestemmelserne i stk. 1.

Det bemærkes i den forbindelse også, at det – selv *hvis* artikel 6, stk. 3, 1. punktum, og ordet "skal" blev tillagt selvstændig betydning i forhold til artikel 6, stk. 1 – fremgår af artikel 6, stk. 3, 1. punktum, at grundlaget skal fremgå af bl.a. "EU-retten", herunder – må man forstå, da der ikke ses at være holdepunkter for andet – f.eks. artikel 6, stk. 1, litra c og e.

Artikel 6, stk. 3, anses på den baggrund først og fremmest "blot" at være en uddybning af kravene til national lovgivning om lovlig behandling af personoplysninger, *hvis* medlemsstaterne udnytter *muligheden* for at vedtage nationale regler efter artikel 6, stk. 2.

Som fortolkningsbidrag til den nærmere forståelse af kravene i artikel 6, stk. 3, fremgår det af præambelbetragtning nr. 41, at når denne forordning henviser til et retsgrundlag eller en lovgivningsmæssig foranstaltning, kræver det ikke nødvendigvis en lov, der er vedtaget af et parlament, med forbehold for krav i henhold til den forfatningsmæssige orden i den pågældende medlemsstat.

Retsgrundlaget kan således f.eks. også fremgå af en bekendtgørelse, fastsat på baggrund af en bemyndigelse i lov, der rummer mulighed for at fastsætte regler om behandling af personoplysninger.

Et sådant retsgrundlag eller en sådan lovgivningsmæssig foranstaltning skal imidlertid efter præambelbetragtningen være klar(t) og præcis(t), og anvendelse heraf bør være forudsigelig for personer, der er omfattet af dets/dens anvendelsesområde, jf. retspraksis fra EU-Domstolen og Den Europæiske Menneskerettighedsdomstol.

Det ses at være i overensstemmelse med gældende ret, at grundlaget for behandling skal fremgå af EU-retten eller af medlemsstaternes nationale ret.

Internationale forpligtelser antages også at falde ind under medlemsstaternes nationale ret, idet internationale forpligtelser må anses som værende blevet en del af en medlemsstats nationale ret efter det enkelte lands forskellige tiltrædelsesregler. Endvidere kan der henvises til, at der i afsnit 3.3. om lovlig behandling af ikke-følsomme oplysninger, artikel 6, stk. 1, omkring litra c anføres, at en retlig forpligtelse også vil være forpligtelser, der følger af internationale regler.

Dernæst fremgår det af artikel 6, stk. 3, at formålet med behandlingen skal være fastlagt i dette retsgrundlag eller for så vidt angår den behandling, der er omhandlet i stk. 1, litra e, være nødvendig for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Dette retsgrundlag kan indeholde specifikke bestemmelser med henblik på at tilpasse anvendelsen af bestemmelserne i denne forordning, bl.a. de generelle betingelser for lovlighed af den dataansvarliges behandling, hvilke typer oplysninger der skal behandles, berørte registrerede, hvilke enheder personoplysninger må videregives til og formålet hermed, formålsbegrænsninger, opbevaringsperioder og behandlingsaktiviteter samt behandlingsprocedurer, herunder foranstaltninger til sikring af lovlig og rimelig behandling såsom i andre specifikke databehandlingssituationer som omhandlet i kapitel IX. EU-retten eller medlemsstaternes nationale ret skal opfylde et formål i samfundets interesse og stå i rimeligt forhold til det legitime mål, der forfølges.

Som fortolkningsbidrag hertil fremgår det af præambelbetragtning nr. 45, at hvis behandling foretages i overensstemmelse med en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, bør behandlingen have retsgrundlag i EU-retten eller medlemsstaternes nationale ret. Denne forordning indebærer ikke, at der kræves en specifik lov til hver enkelt behandling. Det kan være tilstrækkeligt med en lov som grundlag for adskillige databehandlingsaktiviteter, som baseres på en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse.

Det fremgår endvidere af præambelbetragtning nr. 45, at det også bør henhøre under EU-retten eller medlemsstaternes nationale ret at fastlægge formålet med behandlingen. Endvidere kan dette retsgrundlag præcisere denne forordnings generelle betingelser for lovlig behandling af personoplysninger og nærmere præcisere, hvem den dataansvarlige er, hvilken type personoplysninger der skal behandles, de berørte registrerede, hvilke enheder personoplysningerne kan videregives til, formålsbegrænsninger, opbevaringsperiode og andre foranstaltninger til at sikre lovlig og rimelig behandling.

Endelig fremgår det af samme præambelbetragtning, at det ligeledes bør henhøre under EU-retten eller medlemsstaternes nationale ret at afgøre, om den dataansvarlige, der udfører en opgave i samfundets interesse eller i forbindelse med offentlig myndighedsudøvelse, skal være en offentlig myndighed eller en anden fysisk eller juridisk person, der er omfattet af offentlig ret, eller, hvis dette er i samfundets interesse, herunder sundhedsformål, såsom folkesundhed og social sikring samt forvaltning af sundhedsydelser, af privatret som f.eks. en erhvervssammenslutning.

Efter artikel 6, stk. 3, ses medlemsstaterne at have mulighed for at gå relativt langt, idet de med henblik på at tilpasse anvendelsen af bestemmerne i databeskyttelsesforordningen eksempelvis overlades at fastsætte regler om, hvilke type oplysninger, der skal behandles samt hvilke behandlingsprocedurer, der skal efterleves.

Endvidere følger det af artikel 6, stk. 3, at retsgrundlaget *kan* indeholde specifikke bestemmelser med henblik på anvendelsen af bestemmelserne i forordningen, *bl.a*. de generelle betingelser for lovlighed af den dataansvarliges behandling, hvilke typer oplysninger der skal behandles, berørte registrerede, hvilke enheder personoplysninger må videregives til og formålet hermed, formålsbegrænsninger, opbevaringsperioder og behandlingsaktiviteter samt behandlingsprocedurer, herunder foranstaltninger til sikring af lovlig og rimelig behandling såsom i andre specifikke databehandlingssituationer som omhandlet i kapitel IX. Idet bestemmelsen indeholder ordet bl.a., betyder det, at bestemmelsen ikke er udtøm-

mende i forhold til lovgivers mulighed for at fastsætte specifikke regler med henblik på anvendelsen af databeskyttelsesforordningen.

Der må således f.eks. kunne fastsættes bestemmelser om, hvilke enheder personoplysninger ikke må videregives til eller bestemmelser om slettefrister. Der må også kunne fastsættes bestemmelser, som udtømmende opregner, hvilke formål personoplysninger må anvendes til, eller som konkret bestemmer, hvordan personoplysninger skal behandles, f.eks. i kundeforhold eller ved betjening af borgere, drift af e-boks løsninger mv. Alt sammen under forudsætning af, at behandlingshjemlen er forordningens artikel 6, stk. 1, litra c eller e.

Det følger af forordningens artikel 6, stk. 3, 2. pkt., specifikt vedrørende national fastlæggelse af indholdet af en "retlig forpligtelse", at "formålet med behandlingen skal være fastlagt i" det nationale retsgrundlag. Dette krav må antages i en dansk sammenhæng at kunne opfyldes ved, at formålet med behandlingen kan udledes af den pågældende nationale lov med dens forarbejder.

Det følger derudover af forordningens artikel 6, stk. 3, 2. pkt., specifikt vedrørende behandling, der er omhandlet i artikel 6, stk. 1, litra e – dvs. af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse – at behandlingen skal være "nødvendig for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse". Det må også her være tilstrækkeligt for opfyldelse af dette nødvendighedskrav, at det kan udledes af den pågældende nationale lov med dens forarbejder, under forudsætning af at behandlingen rent faktisk er "nødvendig".

I artikel 6, stk. 3, sidste led, er der et yderligere krav til den lovgivning, som tilpasser anvendelsen af databeskyttelsesforordningen. Der er et krav om, at medlemsstaternes nationale ret *skal* opfylde et formål i samfundets interesse og stå i rimeligt forhold til det legitime mål, som forfølges. Databeskyttelsesforordningen fastsætter således et krav om proportionalitet og iagttagelse af samfundets interesse i forbindelse med national ret og EU-ret, der tilpasser anvendelsen af databeskyttelsesforordningen.

Kravet om iagttagelse af samfundets interesse ses dog ikke at være en tilføjelse i forhold til gældende ret, idet hele idéen med lovgivning må være, at den er i samfundets interesse. Kravet om, at lovgivningen skal opfylde et formål i samfundets interesse, må således antages at være opfyldt, når medlemsstaterne vedtager national lovgivning inden for rammerne af forordningens artikel 6, stk. 1, litra c og e.

Derudover må lovgiver også efter gældende ret iagttage et proportionalitetsprincip, når der lovgives, hvilket også særligt fremgår af databeskyttelsesforordningens artikel 5, stk. 1, litra c, hvoraf det fremgår, at behandling af personoplysninger skal være begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

3.4.3.3. Nationalt råderum

Databeskyttelsesforordningens generelle formål, ordlyden i forordningens artikel 6, stk. 2 og 3, samt de relevante præambelbetragtninger indikerer ikke, at det har været hensigten, at der med databeskyttelsesforordningen er tiltænkt et andet rum – end efter databeskyttelsesdirektivet – for at tilpasse anvendelsen af forordningens bestemmelser om behandling ved at fastsætte mere specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling med henblik på overholdelse af artikel 6, stk. 1, litra c og e.

Det vil som anført være medlemsstaterne og EU-lovgiver, som overlades muligheden for at fastsætte, hvornår der er tale om en retlig forpligtelse eller en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, jf. forordningens artikel 6, stk. 1, litra c og e.

Retstilstanden for det nationale råderum ses derfor for så vidt angår anvendelsen af artikel 6, stk. 1, litra c og e, jf. artikel 6, stk. 2-3, at være en videreførelse af gældende ret, ligesom medlemslandene i præambelbetragtning nr. 10 overlades muligheden for at *opretholde* nationale bestemmelser for yderligere at præcisere bestemmelserne i forordningen.

Det følger af bestemmelserne i artikel 6, stk. 2 og 3, at disse også finder anvendelse for kapitel 9, det vil sige databeskyttelsesforordningens kapitel om specifikke behandlingssituationer vedrørende ytrings- og informationsfrihed, aktindsigt, nationalt identifikationsnummer, ansættelsesforhold, arkivformål, tavshedspligt og kirkers og religiøse sammenslutningers databeskyttelsesregler. At kapitel 9 nævnes i artikel 6, stk. 2 og 3, betyder, at det også ved behandling i de specifikke behandlingssituationer vil være muligt at opretholde eller indføre mere specifikke bestemmelser for at tilpasse anvendelsen af databeskyttelsesforordningens bestemmelser.

Hverken i databeskyttelsesforordningen eller i præambelbetragtningerne hertil er der bestemmelser, som svarer til persondatalovens § 2, stk. 1, hvorefter regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i denne lov.

Efter databeskyttelsesforordningen vil vurderingen af lovligheden af en behandling således skulle tage sit udgangspunkt i forordningen, der som nævnt giver mulighed for nationalt at

fastsætte yderligere betingelser for lovlig behandling, f.eks. at fastsætte en retlig forpligtelse.

Hjemlen til at fastsætte særregler vil herefter skulle findes i artikel 6, stk. 2 og 3, som henviser til artikel 6, stk. 1, litra c og e, og for følsomme oplysninger således i artikel 9, stk. 2-4.

For særlovgivningen vil dette betyde, at medlemsstaterne kan *opretholde* nationale bestemmelser for yderligere at præcisere anvendelsen af forordningens bestemmelser. Således vil eksisterende lovgivning, som i forbindelse med udarbejdelsen af lovforslaget eller bekendtgørelsen blev vurderet som værende i overensstemmelse med databeskyttelsesdirektivet, antageligvis kunne bestå.

Disse nationale særregler vil endvidere skulle overholde forordningens øvrige bestemmelser, herunder særligt artikel 5 om principper for behandling af personoplysninger.

I Danmark er der vedtaget en betydelig mængde særlovgivning og særlige bestemmelser om lovlig behandling af personoplysninger i både den offentlige og private sektor, bl.a. bestemmelser i lov om det centrale personregister, lov om finansiel virksomhed, lov om betalingstjenester og elektroniske penge, skattekontrolloven, lov om retssikkerhed og administration på det sociale område, offentlighedsloven og sundhedsloven.

Persondataloven indeholder i sig selv alene bestemmelser om, hvornår behandling *kan eller må* finde sted, hvorimod en række særregler, som eksempelvis skattekontrolloven, indeholder bestemmelser, hvorefter der *skal* ske behandling. Når forordningen finder anvendelse, er den både udgangspunktet for, hvornår behandling *kan eller må* finde sted, mens den også udgør et grundlag for nationale regler om, hvornår behandling *kan eller må* ske, og hvornår behandling *skal* ske, idet sådanne nationale regler eksempelvis vil have hjemmel i forordningens artikel 6, stk. 1, litra c.

Eksempelvis må det antages, at bestemmelser i skattekontrolloven om arbejdsgiveres pligt til at indsamle og indberette forskellige økonomiske oplysninger om den ansatte til skattemyndighederne vil kunne opretholdes, når forordningen får virkning. Forordningen er således ikke til hinder for en national bestemmelse om, hvornår behandling skal ske.

Der må endvidere antages at være adgang til at opretholde eller indføre konkrete lovregler – inden for rammerne af forordningens artikel 6, stk. 2-3 – om f.eks. behandling af oplysninger i den finansielle sektor, såsom reglerne i kapitel 9 i lov om finansiel virksomhed om videregivelse af fortrolige oplysninger og betalingstjenestelovens § 85, omtalt ovenfor,

eller i sundhedssektoren. Der kan således også for behandling i den private sektor, ligesom i forhold til behandling i den offentlige sektor, ske behandling af personoplysninger, hvis det sker for at overholde en "retlig forpligtelse", som påhviler den dataansvarlige (artikel 6, stk. 1, litra c), eller hvis lovgiver i øvrigt har udnyttet sin mulighed for nationalt at fastlægge, hvornår det skal være – og ikke skal være – muligt at behandle personoplysninger af hensyn til "samfundets interesse" (artikel 6, stk. 1, litra e).

I medfør af artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2-3, vil det endvidere være muligt at regulere behandlingen af personoplysninger i forbindelse med forhold, der under gældende ret anses for at vedrøre myndighedsudøvelse f.eks. kommunale myndigheders afgørelsesvirksomhed. Der vil således bl.a. kunne fastsættes nærmere regler om, hvilke oplysninger, der skal indsamles, videregives mv. i forbindelse med en myndigheds sagsbehandling, samt hvilke modtagere oplysninger kan videregives til med henblik på videreanvendelse af oplysningerne hos modtageren.

Muligheden for at opretholde eller indføre yderligere betingelser er dog begrænset af, at det ikke bør hæmme den frie udveksling af personoplysninger i EU, når disse betingelser finder anvendelse på grænseoverskridende behandling af sådanne oplysninger. Dette krav må i praksis navnlig antages at have relevans for regulering, der direkte er rettet mod den private sektor, eller i væsentlig grad påvirker denne, idet hensynet til den fri bevægelighed må antages i praksis at have mere begrænset betydning for den offentlige sektor. Dog vil ethvert relevant lovgivningsmæssigt tiltag mv. skulle vurderes i forhold til dette krav, uanset om det er rettet mod den private eller offentlige sektor.

3.4.3.4. Offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv.
Det har været overvejet i hvilket omfang offentlige myndigheder kan offentliggøre kontrol- og analyseresultater og afgørelser mv. om personer og/eller virksomheder i identificerbar form. Denne form for offentliggørelse – der i stigende grad sker via internettet – omfatter i mange tilfælde oplysninger, der ellers ville være fortrolige, herunder oplysninger om f.eks. personer eller virksomheder, der ikke har overholdt regler fastsat i lovgivningen.

Personoplysninger, som er omfattet af retten til aktindsigt efter offentlighedsloven, kan af egen drift offentliggøres af myndigheder, jf. herved den udtalelse, der er gengivet i Folketingets Ombudsmands beretning for 1996, side 51 ff. En forvaltningsmyndighed vil dog i denne sammenhæng skulle agere inden for rammerne af god forvaltningsskik og de almin-

delige forvaltningsretlige principper om saglighed og proportionalitet samt ved oplysninger om fysiske personer inden for rammerne af persondataloven.[182]

Det antages, at der kun yderst sjældent vil være hjemmel til, at en myndighed af egen drift uden særskilt hjemmel i en særlov, kan offentliggøre kontrolresultater, afgørelser mv., som indeholder personoplysninger omfattet af persondatalovens § 7. Personoplysninger omfattet af § 8 kan i et vist videre omfang offentliggøres. Det vil efter persondatalovens § 8, stk. 2, nr. 2, være muligt, hvis det konkret sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, som begrunder hemmeligholdelse, herunder hensynet til den, som oplysningen angår. Desuden vil ikke-fortrolige og almindeligt fortrolige oplysninger i en række tilfælde efter en konkret vurdering kunne offentliggøres med hjemmel i persondatalovens § 6, stk. 1, nr. 3, 5, 6 eller 7.[183]

Som eksempler på lovbestemte offentliggørelsesordninger kan nævnes Disciplinær- og klagenævnet for beskikkede bygningssagkyndiges offentliggørelse af bl.a. navnene på bygningssagkyndige, der er blevet tildelt en advarsel eller har fået inddraget beskikkelsen som følge af alvorlige eller gentagne fejl i tilstandsrapporter og Styrelsen for Patientsikkerheds offentliggørelse på internettet af bl.a. navnene på autoriserede sundhedspersoner, der enten er under skærpet tilsyn, har fået påbud eller har fået foretaget ændringer i deres autorisationsforhold.

Det vurderes i betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv., at reglerne i persondataloven fører til, at der kun kan etableres ordninger med systematisk offentliggørelse af kontrolresultater, afgørelser mv. i ikke-anonymiseret form, hvis der er særlig og klar lovhjemmel hertil.[184]

Betænkningen beskriver også vægtningen af de hensyn, der skal afvejes overfor hinanden ved etablering af sådanne offentliggørelsesordninger, nemlig på den ene side hensynet bag ordningen (betænkningens s. 114-117) og på den anden side hensynet til de personer, som de oplysninger, der vil kunne blive offentliggjort, vedrører (betænkningens s. 111-114).

Betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. munder ud i en "tjekliste", som myndigheder, der overvejer ved eller i henhold til lov at indføre nye ordninger med systematisk offentliggørelse af oplysninger

[182] Betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv., s. 64.
[183] Betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv., s. 64.
[184] Betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv., s. 64 og 107 f.

om kontrolresultater og afgørelser mv. på internettet i ikke-anonymiseret form, forinden bør anvende.[185]

Efter afgivelsen af betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. fandt EU-Domstolen i sag C-92/09 og C-93/09, Volker und Markus Schecke GbR & Hartmut Eifert, dom af 9. november 2010, at offentliggørelse af navne på alle de fysiske personer, der havde modtaget støtte fra landbrugsfonde, samt de nøjagtige beløb, som disse havde modtaget, overskred de grænser, som en overholdelse af EU-proportionalitetsprincippet opstillede. Sagen drejede sig om den tyske forbundsmyndighed for landbrug og fødevares offentliggørelse på sin hjemmeside af oplysninger om modtagere af landbrugsstøtte fra fondene EGFL og ELFUL. EU-Domstolen fastslog i sagen, at den ordning, som fulgte af de forordninger, som offentliggørelse skete i henhold til, udgjorde et indgreb i de pågældende støttemodtageres rettigheder som fastlagt i EU-charterets artikel 7 og 8.

Det fremgår af dommens præmis 86, at det ikke fremgik, at institutionerne havde foretaget en rimelig afvejning mellem på den ene side formålene i artikel 44a i forordning nr. 1290/2005 og i forordning nr. 259/2008 og på den anden side de rettigheder, som for fysiske personer er anerkendt i chartrets artikel 7 og 8. Under hensyntagen til den omstændighed, at undtagelser fra og begrænsninger af beskyttelsen af personoplysninger skulle holdes inden for det strengt nødvendige, og at det var muligt at tænke sig foranstaltninger, der for de fysiske personer greb mindre ind i nævnte grundlæggende rettighed, mens de samtidig bidrog effektivt til at opfylde formålene i den omhandlede EU-lovgivning, måtte det fastslås, at Rådet og Kommissionen ved at indføre en offentliggørelse af navne på alle de fysiske personer, der havde modtaget midler fra EGFL og ELFUL, samt de nøjagtige beløb, som disse havde modtaget, havde overskredet de grænser, som en overholdelse af proportionalitetsprincippet opstillede.

I dommen havde lovgiver således konkret ikke foretaget en proportionalitetsvurdering.

Dommen slår fast, at de enkelte offentliggørelsesordninger, som i dag findes i dansk ret, vil skulle leve op til de krav, som følger af EU-proportionalitetsprincippet, i det omfang ordningerne er omfattet af EU-rettens anvendelsesområde, herunder databeskyttelsesforordningen og databeskyttelsesdirektivet.[186]

[185] Betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv., s. 15 og 122.
[186] Persondataloven med kommentarer, (2015), s. 49.

Efter databeskyttelsesforordningen er der ikke et udtrykkeligt krav om, at der skal være udtrykkelig lovhjemmel for, at der kan etableres en ordning med systematisk offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke-anonymiseret form.

Da offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke-anonymiseret form vil være en indgribende behandlingssituation, vil sådan behandling dog skærpe opmærksomheden på kravene i blandt andet forordningens artikel 5 om principper for behandling af personoplysninger, herunder proportionalitetsprincippet.[187]

Databeskyttelsesforordningen ses ikke at ændre afgørende ved den beskrevne retsstilling i betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. Det må således også efter databeskyttelsesforordningen antages, at det skaber det sikreste behandlingsgrundlag for systematisk offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke-anonymiseret form, hvis der ligger en særlig og klar national lovhjemmel til grund for offentliggørelsen – udarbejdet i overensstemmelse med forordningens rammer for national lovgivning, jf. bl.a. artikel 6, stk. 2-3.

Når forordningen finder anvendelse den 25. maj 2018, må det antages, at det er muligt – i forarbejderne til en ny udgave af persondataloven – at operere med en forudsætning om, at der skal ligge en særlig og klar lovhjemmel til grund for systematisk offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke-anonymiseret form.

3.4.4. Overvejelser

Medlemsstaternes mulighed for at opretholde og indføre mere specifikke bestemmelser for behandling af ikke-følsomme oplysninger for at tilpasse anvendelsen af databeskyttelsesforordningen vil overordnet ikke være en ændring i forhold til gældende ret. Dette også i forhold til særlovgivningen.

Dog vil det efter databeskyttelsesforordningen kun være muligt at opretholde og indføre mere specifikke bestemmelser for at tilpasse anvendelsen i forbindelse med artikel 6, stk. 1, litra c og e, hvorfor der ikke for så vidt angår artikel 6, stk. 1, litra a, b, d og f, vil være muligt at tilpasse anvendelsen – dette vil dog som anført ikke få den store praktiske betydning.

[187] Dette følger også af EU-Domstolens afgørelse i sag C-92/09 og C-93/09, Volker und Markus Schecke GbR & Hartmut Eifert.

3.4.4.1."Tjekliste" for bedømmelse af eksisterende nationale særregler vedrørende ikke-følsomme oplysninger om behandlings forenelighed med databeskyttelsesforordningen
Denne tjekliste vedrører muligheden for at opretholde regler for *lovlig behandling* i overensstemmelse med artikel 6. Tjeklisten medtager således ikke andre og mere specifikke krav, som den nationale lovgiver også skal være opmærksom på, som eksempelvis den registreredes rettigheder og begrænsninger heraf, jf. artikel 23, artikel 26 om fælles dataansvarlige og artikel 28 om databehandler. For nærmere herom henvises bl.a. til afsnit 4.13. om begrænsninger af rettigheder, artikel 23.

Når myndigheder skal overveje, hvorvidt eksisterende nationale særregler kan *opretholdes*, når databeskyttelsesforordningen finder anvendelse, anbefales følgende punkter sammenfattende iagttaget i forhold til vurderingen af, om der er hjemmel til behandlingen:

Det skal bemærkes, at det må antages, at de eksisterende danske særregler om behandling af ikke-følsomme oplysninger normalt som tidligere anført vil kunne bestå.

1. Det kan indledningsvis overvejes, om den nationale regel fortsat ønskes opretholdt, eller om behandling fremover skal ske alene efter behandlingsreglerne i databeskyttelsesforordningen.

I den forbindelse kan det indgå i vurderingen, om retsområdet kan administreres alene og direkte på grundlag af behandlingsreglerne i forordningens artikel 6, stk. 1, litra e, om udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse.

I det omfang det foreslås at opretholde nationale særregler, der har erhvervsøkonomiske konsekvenser for danske virksomheder, skal der tages stilling til, om principperne for implementering af erhvervsrettet EU-regulering i Danmark efterleves. Hvis principperne ikke efterleves, og den opretholdte regel indgår i et forslag til en ny lov eller bekendtgørelse, skal der forelægges en sag for Implementeringsudvalget.[188]

2. Dernæst bør det vurderes, hvorvidt hjemlen til den eksisterende regel kan findes i forordningens artikel 6, stk. 1, litra c, jf. artikel 6, stk. 2-3, hvorefter behandlingen skal være nødvendig for at overholde en *retlig forpligtelse*, som påhviler den dataansvarlige,

[188] Se nærmere på Beskæftigelsesministeriets hjemmeside.

eller i forordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2-3, hvorefter behandlingen er nødvendig af hensyn til udførelse af en opgave i *samfundets interesse* eller som henhører under *offentlig myndighedsudøvelse*, som den dataansvarlige har fået pålagt.

3. Dernæst skal det vurderes, hvorvidt den eksisterende regel lever op til kravet om at være en mere specifik bestemmelse om anvendelse af forordningen, ved at fastsætte mere præcist specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling i overensstemmelse med forordningens artikel 6, stk. 2.

4. Endvidere skal der sørges for specifikt vedrørende en retlig forpligtelse, at formålet med behandlingen skal være fastlagt i det nationale retsgrundlag, jf. artikel 6, stk. 3, 2. pkt. Dette krav må antages at kunne opfyldes ved, at formålet med behandlingen kan udledes af pågældende lov med dens forarbejder,

eller specifikt vedrørende behandling, der er omhandlet i artikel 6, stk. 1, litra e – dvs. af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse – at behandlingen skal være nødvendig for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, jf. artikel 6, stk. 3, 2. pkt. Det må også her være tilstrækkeligt for opfyldelse af dette nødvendighedskrav, at det kan udledes af pågældende lov med dens forarbejder.

5. Derudover skal det iagttages, at reglen skal være proportional, jf. forordningens artikel 6, stk. 3, sidste pkt., og artikel 5, stk. 1, litra c. Endvidere skal reglen opfylde et formål i samfundets interesse, hvilket må antages at være opfyldt allerede i og med, at Folketinget vedtager en lov eller en bemyndigelse i en lov, jf. forordningens artikel 6, stk. 3, sidste pkt.

Samtidig skal reglen overholde principperne for behandling i forordningens artikel 5, hvilket eksempelvis betyder, at lovgivningen ikke må medføre, at der sker en opbevaring i strid med artikel 5, stk. 1, litra e.

6. Endelig skal det sikres, at der er den rette balance i forhold til den fri bevægelighed for personoplysninger, jf. forordningens artikel 1.

3.4.4.2. "Tjekliste" ved udarbejdelse af nye nationale særregler for behandling af ikke-følsomme personoplysninger

Denne tjekliste vedrører muligheden for at fastsætte regler for lovlig behandling i overensstemmelse med artikel 6. Tjeklisten medtager således ikke andre og mere specifikke krav, som den nationale lovgiver også skal være opmærksom på, som eksempelvis den registre-

redes rettigheder og begrænsninger heraf, jf. artikel 23, artikel 26 om fælles dataansvarlige og artikel 28 om databehandler.

Når myndigheder fremadrettet overvejer at udfærdige nationale særregler efter det nationale råderum, som databeskyttelsesforordningen efterlader i artikel 6, stk. 2-3, anbefales følgende punkter sammenfattende iagttaget i forhold til vurderingen af, om der er hjemmel til behandlingen:

1. Det kan indledningsvis overvejes, om der overhovedet ønskes fastsat en national regel, eller om behandling fremover skal ske alene efter behandlingsreglerne i databeskyttelsesforordningen. Forordningens behandlingshjemmel i artikel 6, stk. 1, litra e, kan således i mange tilfælde benyttes som direkte hjemmel til behandlingen, hvilket artikel 6, stk. 1, litra c, også kan så længe der er en retlig forpligtelse, der fremgår af EU-retten eller national ret.

I det omfang, det foreslås at indføre nationale særregler, der har erhvervsøkonomiske konsekvenser for danske virksomheder, skal der tages stilling til, om principperne for implementering af erhvervsrettet EU-regulering i Danmark efterleves. Hvis principperne ikke efterleves, skal der forelægges en sag for Implementeringsudvalget.[189]

2. Såfremt det vurderes nødvendigt eller ønskeligt, skal der findes hjemmel til den nationale særregel i forordningens artikel 6, stk. 1, litra c, jf. artikel 6, stk. 2-3, hvorefter behandlingen skal være nødvendig for at overholde en *retlig forpligtelse*, som påhviler den dataansvarlige,

eller der skal findes hjemmel til den nationale særregel i forordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2-3, hvorefter behandlingen er nødvendig af hensyn til udførelse af en opgave i *samfundets interesse* eller som henhører under *offentlig myndighedsudøvelse*, som den dataansvarlige har fået pålagt.

3. Dernæst skal det vurderes, hvorvidt særreglen indfører mere specifikke bestemmelser for at tilpasse anvendelsen ved at fastsætte mere præcist specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling i overensstemmelse med forordningens artikel 6, stk. 2.

4. Endvidere skal der sørges for specifikt vedrørende en retlig forpligtelse, at formålet med behandlingen skal være fastlagt i det nationale retsgrundlag, jf. artikel 6, stk. 3, 2. pkt. Dette krav må antages at kunne opfyldes ved, at formålet med behandlingen kan udledes af

[189] Se nærmere på Beskæftigelsesministeriets hjemmeside.

pågældende lov med dens forarbejder, under forudsætning af at behandlingen rent faktisk er "nødvendig".

eller specifikt vedrørende behandling, der er omhandlet i artikel 6, stk. 1, litra e – dvs. af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse – skal der sørges for, at behandlingen skal være nødvendig for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, jf. artikel 6, stk. 3, 2. pkt. Det må også her være tilstrækkeligt for opfyldelse af dette nødvendighedskrav, at det kan udledes af pågældende lov med dens forarbejder.

5. Derudover skal det iagttages, at reglen skal være proportional, jf. forordningens artikel 6, stk. 3, sidste pkt. og artikel 5, stk. 1, litra c. Endvidere skal reglen opfylde et formål i samfundets interesse, hvilket må antages at være opfyldt allerede i og med, at Folketinget vedtager en lov eller en bemyndigelse i en lov, jf. forordningens artikel 6, stk. 3, sidste pkt.

Samtidig skal lovgivningen indrettes, så behandlingen kan ske i overensstemmelse med principperne for behandling i forordningens artikel 5, hvilket eksempelvis betyder, at lovgivningen ikke må medføre, at der sker en opbevaring i strid med artikel 5, stk. 1, litra e.

6. Endelig skal det sikres, at der er den rette balance i forhold til den fri bevægelighed for personoplysninger, jf. forordningens artikel 1.

3.5. Betingelser for samtykke, artikel 7

3.5.1. Præsentation

Persondataloven, databeskyttelsesdirektivet og databeskyttelsesforordningen indeholder regler for, hvornår personoplysninger kan behandles, og det følger heraf som altovervejende hovedregel, at personoplysninger vil kunne behandles, såfremt der er det fornødne samtykke fra den registrerede til behandlingen. Samtykke bruges således i vidt omfang som behandlingshjemmel, som én blandt flere mulige ligestillede behandlingshjemler.

Persondataloven indeholder i § 3, nr. 8, en definition af samtykke fra den registrerede. Endvidere indeholder databeskyttelsesforordningen i artikel 4, nr. 11, en lignende definition af den registreredes samtykke.

I forordningen er der endvidere i artikel 7 indsat en præcisering af betingelserne for samtykke i forordningen.

3.5.2. Gældende ret

Det følger af persondatalovens § 3, nr. 8, at ved den registreredes samtykke forstås enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

Ordlyden i persondatalovens § 3, nr. 8, er identisk med den tilsvarende bestemmelse i artikel 2, litra h, i databeskyttelsesdirektivet, som endvidere i artikel 7, litra a, indeholder en bestemmelse om, at behandling på baggrund af samtykke kun må finde sted, hvis der ikke hersker tvivl om, at den registrerede har givet samtykke.

Den tidligere gældende registerlovgivning indeholdt ikke en legal definition af begrebet samtykke.

3.5.2.1. Bevisbyrden for gyldigt samtykke

Bevisbyrden for, at der foreligger et samtykke fra en registreret, vil efter gældende ret påhvile den dataansvarlige.[190] Ifølge bemærkningerne til persondataloven gælder der ikke noget formkrav til et samtykke. Der kan således være tale om såvel skriftligt som mundtligt samtykke fra den registrerede, ligesom samtykket også vil kunne gives digitalt. Da bevisbyrden for, at der foreligger et samtykke, som opfylder lovens krav, påhviler den dataansvarlige, anbefales det dog, at et samtykke i videst muligt omfang afgives skriftligt.[191]

Datatilsynet udtalte i Sarbanes Oxley Act-sagen, at samtykkekravet ikke indebærer et egentligt krav om skriftlighed, men at dette kan være hensigtsmæssigt af hensyn til bevisbyrden.[192] Det vil især være af betydning, hvorvidt der er indhentet et skriftligt samtykke i de tilfælde, hvor der sker behandling af oplysninger, som er af følsom karakter, eller hvis samtykket i øvrigt har stor betydning for en eller flere af parterne.

I forhold til offentlige myndigheders behandling af personoplysninger, kan det anføres, at der ved afgivelse af mundtligt samtykke efter lov om offentlighed i forvaltningen[193] og et almindeligt forvaltningsretligt princip vil skulle gøres notat om samtykket.[194]

---

[190] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3, og Persondataloven med kommentarer (2015), s. 170.
[191] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.
[192] Sarbanes Oxley Act-sagen, Datatilsynets j.nr. 2003-233-0028.
[193] Lov om offentlighed i forvaltningen, jf. lov nr. 606 af 12. juni 2013.
[194] Persondataloven med kommentarer (2015), s. 170.

3.5.2.2. Informeret samtykke

Det fremgår af bemærkningerne til persondataloven, at et samtykke skal være informeret i den forstand, at den samtykkende skal være klar over, hvad det er, vedkommende meddeler samtykke til. Den dataansvarlige må således sikre sig, at der gives den registrerede tilstrækkelig information til, at den pågældende kan vurdere, hvorvidt samtykke bør meddeles.[195]

Artikel 29-gruppen udtaler i den forbindelse, at behovet for, at samtykket er "informeret", afføder to yderligere krav.[196] For det første skal den måde, hvorpå informationerne meddeles, sikre, at der anvendes et egnet sprog, så de registrerede forstår, hvad de samtykker i, herunder til hvilke formål. Anvendelse af en alt for kompliceret retlig eller teknisk jargon lever ikke op til kravene i lovgivningen. For det andet skal de informationer, der meddeles de registrerede, være klare og tilstrækkeligt synlige, så de registrerede ikke overser dem, ligesom informationerne skal afgives direkte til dem.

3.5.2.3. Tilbagekaldelse af samtykke

Det fremgår af persondatalovens § 38, at den registrerede kan tilbagekalde et samtykke.

I forbindelse med vedtagelsen af persondataloven, blev det i lovens § 38 præciseret, at samtykke kan tilbagekaldes. Dette skete for at tydeliggøre og forbedre den beskyttelse, som den registrerede sikres gennem reglerne i loven.[197] Der er således i persondataloven indsat en særlig bestemmelse i § 38, som ikke findes tilsvarende i databeskyttelsesdirektivet. Artikel 29-gruppen har dog udtalt, at kravet om muligheden for at tilbagekalde et samtykke følger implicit af databeskyttelsesdirektivet.[198] Artikel 29-gruppen præciserer, at det er vigtigt, at personer, som har givet samtykke, har mulighed for at tilbagekalde dette samtykke.[199]

Det fremgår af bemærkningerne til persondataloven, at den registrerede på et hvilket som helst tidspunkt kan tilbagekalde et samtykke. Et samtykke kan dog ikke tilbagekaldes med tilbagevirkende kraft. Virkningen af tilbagekaldelse vil derfor være, at den behandling af oplysninger, som den registrerede har meddelt sit samtykke til, normalt ikke må finde sted fremover.[200] Artikel 29-gruppen har ligeledes udtalt, at tilbagetrækning af et samtykke ikke

[195] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.
[196] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s. 38.
[197] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 38.
[198] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s. 32.
[199] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s. 34.
[200] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.

har tilbagevirkende kraft, men at en tilbagetrækning af samtykke skal forhindre, at den dataansvarlige foretager yderligere behandling af oplysningerne.[201]

Artikel 29-gruppen har udtalt, at det vil være hensigtsmæssigt, såfremt den nye databeskyttelseslovgivning indeholder en eksplicit klausul, hvoraf det fremgår, at registrerede har ret til at trække deres samtykke tilbage.[202]

I dansk ret er der ikke en udtrykkelig bestemmelse, som fastslår, at inden samtykke gives, skal der ske oplysning af den registrerede om, at samtykket kan trækkes tilbage. Det kan dog ikke udelukkes, at denne retstilstand ville kunne blive resultatet efter en konkret vurdering efter gældende ret. Efter gældende ret ville et sådant krav til samtykkets gyldighed kunne følge af god databehandlingsskik, af selve kravet til et informeret samtykke eller eventuelt af oplysningspligten for den dataansvarlige efter persondatalovens §§ 28 og 29. Hertil skal det bemærkes, at i kravet om, at et samtykke skal være informeret, er der et krav om, at der skal gives yderligere information i det omfang, den konkrete situation tilsiger dette.[203]

Der ses dog ikke i gældende ret eksplicit at være taget stilling til, om der helt overordnet generelt gælder en pligt til at informere om, at samtykke kan trækkes tilbage. I Sarbanes Oxley Act-sagen udtalte Datatilsynet dog følgende: *"Persondatalovens definition af samtykke i § 3, nr. 8, ifølge hvilken et samtykke skal være "informeret", må derfor som minimum forudsætte, at arbejdstageren informeres om, hvorvidt tilbagekaldelse reelt er muligt eller ej."*[204] I denne sag lagde Datatilsynet således til grund, at den registrerede skulle oplyses om, hvorvidt tilbagekaldelsen var mulig.

3.5.2.4. Frivilligt samtykke

Den registreredes samtykke skal være frivilligt, jf. persondatalovens § 3, nr. 8. Samtykket må ikke være afgivet under tvang. Dette gælder, uanset om det er den dataansvarlige selv eller andre, der øver pression over for den registrerede.[205]

Den omstændighed, at den registrerede er i den dataansvarliges varetægt, f.eks. indsat i fængsel, undergivet værnepligt mv., udelukker ikke, at vedkommende kan give et gyldigt samtykke.[206]

---

[201] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s. 9.
[202] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s. 37.
[203] Persondataloven med kommentarer (2015), s. 174.
[204] Sarbanes Oxley Act-sagen, Datatilsynets j.nr. 2003-233-0028.
[205] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3.
[206] Persondataloven med kommentarer (2015), s. 171-172.

Der kan dog opstå situationer, hvor der kan rejses spørgsmål om, hvorvidt et afgivet samtykke er frivilligt. Eksempelvis kan nævnes den omstændighed, at den registrerede opnår en modydelse for at afgive samtykke. Såfremt det er en forudsætning for at erhverve en offentlig ydelse, at den registrerede samtykker til en bestemt databehandling, kunne det anføres, at samtykket ikke er frivilligt. En sådan antagelse kan dog ikke anses for at være gældende generelt.[207] Datatilsynet udtalte i Sarbanes Oxley Act-sagen, at den omstændighed, at et samtykke skal være frivilligt betyder, at samtykket ikke må være undergivet tvang. Det er derimod fast antaget i såvel teori som i praksis, at den omstændighed, at den registrerede opnår en modydelse, herunder en offentligretlig ydelse, ikke bevirker, at et samtykke ikke kan anses for at være afgivet frivilligt.[208]

Såfremt det er en forudsætning for at erhverve en vare, at den registrerede samtykker til en bestemt databehandling, kunne det overvejes, hvorvidt samtykket bør anses som værende afgivet frivilligt. Dette ses dog ikke at være gældende ret. Et samtykke må således generelt anses for frivilligt, selv om det er afgivet af den registrerede som følge af, at den dataansvarlige ellers ikke ville indgå i et kontraktforhold med den pågældende.[209]

Artikel 29-gruppen udtaler vedrørende definitionen af samtykke, at der ikke må være væsentlige negative konsekvenser for den registrerede, hvis denne ikke samtykker.[210] Databehandling i ansættelsessammenhæng, hvor der er et underordnelsesforhold og i forbindelse med ydelser fra det offentlige, f.eks. inden for sundhedsområdet, kan kræve en nøje vurdering af, om der er tale om et frivilligt samtykke fra de ansattes/borgerens side.

Peter Blume har anført, at forudsætningen om frivillighed ikke er nogen ideel norm. Han anfører, at på et vigtigt område som arbejdsmarkedet er det i mange tilfælde noget af en illusion, at ansatte, der står i et afhængighedsforhold til deres arbejdsgiver, kan give et reelt frivilligt samtykke.[211]

Artikel 29-gruppen har ligeledes udtalt, at der er behov for ikke at tillægge samtykke som behandlingshjemmel for stor betydning, således at samtykke ikke altid er det primære eller den mest ønskelige hjemmel for behandling af personoplysninger.[212] Andre behandlingshjemler kan i stedet overvejes.

[207] Persondataloven med kommentarer (2015), s. 171.
[208] Sarbanes Oxley Act-sagen, Datatilsynets j.nr. 2003-233-0028.
[209] Persondataloven med kommentarer (2015), s. 171.
[210] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s. 38.
[211] Peter Blume, Behandling af persondata – en kritisk kommentar, 1. udgave, 2003, s. 73.
[212] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s.10.

I sag C-291/12, Michael Schwarz, af 17. oktober 2013, udtalte EU-Domstolen sig om samtykke i forbindelse med artikel 8, stk. 2, i EU's charter om grundlæggende rettigheder. I sagen udtalte domstolen, at EU-borgere, der ønskede at ansøge om pas, i den pågældende situation ikke kunne modsætte sig behandlingen af deres fingeraftryk, hvorfor borgerne ikke kunne anses for at have givet samtykke til behandlingen.

Det fremgår af persondataloven med kommentarer, at selvom dommen angår betydningen af EU-charterets artikel 8, stk. 2, er det nærliggende at antage, at EU-Domstolen i en tilsvarende situation vil anlægge samme betragtning i forhold til de samtykkeregler, som følger af databeskyttelsesdirektivet. Det er dog samtidig vigtigt at være opmærksom på, at dommen alene angår den i pasforordningen foreskrevne brug af biometri i forbindelse med udstedelse af pas og rejsedokumenter. Der bør derfor udvises forsigtighed med at slutte fra EU-Domstolens betragtninger i den nævnte situation og til andre situationer, hvor den berørte person konkret kan opleve at være nødt til at give samtykke til, at der kan behandles oplysninger om vedkommende, for at kunne opnå en aftale, fordel mv.[213]

Artikel 29-gruppen udtaler, at samtykke kun vil være gyldigt, hvis den registrerede er i stand til at udøve et reelt valgt, og der ikke er nogen risiko for negative konsekvenser, hvis der ikke gives samtykke. Hvis et samtykke underminerer et individs ret til et frit valg, vil samtykke ikke være frit.

Artikel 29-gruppen udtaler endvidere, at dette kan eksemplificeres i det tilfælde, hvor den registrerede er under indflydelse fra den dataansvarlige, som for eksempel en arbejdsgiver. Hvis arbejdstageren ikke har mulighed for at sige nej, er der ikke tale om et samtykke. I de tilfælde, hvor manglende afgivelse af et samtykke vil kunne betyde, at den registrerede mister en jobmulighed, vil der ikke være tale om et gyldigt samtykke. Selv om der kan være en stærk formodning om, at samtykket er svagt i sådanne sammenhænge, udelukker det ikke helt dets anvendelse, forudsat at der er tilstrækkelige garantier for, at samtykket reelt er frivilligt.[214]

Artikel 29-gruppen har endvidere udtalt, at når en arbejdsgiver finder, at det vil være nødvendigt at behandle personoplysninger, vil det være misledende, hvis behandlingshjemlen hertil findes i opnåelse af et samtykke fra den ansatte. En arbejdsgiver bør kun behandle personoplysninger på baggrund af et samtykke, hvis den ansatte har et reelt frit valg, og senere vil kunne tilbagekalde samtykket uden at lide skade.[215]

[213] Persondataloven med kommentarer (2015), s. 172.
[214] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s.13-15.
[215] Artikel 29-gruppens udtalelse nr. 8/2001 om behandling af personoplysninger i ansættelsesforhold (WP 48), s. 3.

3.5.3. Databeskyttelsesforordningen

I forordningens artikel 4, nr. 11, er samtykke fra den registrerede defineret som enhver frivillig, specifik, informeret og utvetydig viljetilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling.

Hertil fremgår det af præambelbetragtning nr. 32, at samtykke bør gives i form af en klar bekræftelse, der indebærer en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved vedkommende accepterer, at personoplysninger om vedkommende behandles, f.eks. ved en skriftlig erklæring, herunder elektronisk, eller en mundtlig erklæring. Dette kan f.eks. foregå ved at sætte kryds i et felt ved besøg på et websted, ved valg af tekniske indstillinger til informationssamfundstjenester eller en anden erklæring eller handling, der tydeligt i denne forbindelse tilkendegiver den registreredes accept af den foreslåede behandling af vedkommendes personoplysninger. Tavshed, forudafkrydsede felter eller inaktivitet bør derfor ikke udgøre samtykke. Samtykke bør dække alle behandlingsaktiviteter, der udføres til det eller de samme formål. Når behandling tjener flere formål, bør der gives samtykke til dem alle. Hvis den registreredes samtykke skal gives efter en elektronisk anmodning, skal anmodningen være klar, kortfattet og ikke unødigt forstyrre brugen af den tjeneste, som samtykke gives til.

Det fremgår endvidere af præambelbetragtning nr. 33, at det ofte ikke er muligt fuldt ud at fastlægge formålet med behandling af personoplysninger til videnskabelige forskningsformål, når oplysninger indsamles. De registrerede bør derfor kunne give deres samtykke til bestemte videnskabelige forskningsområder, når dette er i overensstemmelse med anerkendte etiske standarder for videnskabelig forskning. Registrerede bør have mulighed for kun at give deres samtykke til bestemte forskningsområder eller dele af forskningsprojekter i det omfang, det tilsigtede formål tillader det.

Forordningens artikel 7 indeholder en præcisering af betingelserne for samtykke, således at stk. 1 handler om, at den dataansvarlige skal kunne påvise eksistensen af et samtykke, mens stk. 2-4 opstiller yderligere betingelser – udover definitionen i artikel 4, nr. 11 – for, at samtykket er gyldigt.

3.5.3.1. Databeskyttelsesordningens artikel 7, stk. 1

Det følger af forordningens artikel 7, stk. 1, at hvis behandling er baseret på samtykke, skal den dataansvarlige kunne påvise, at den registrerede har givet samtykke til behandling af sine personoplysninger. I præambelbetragtningerne til forordningen er der ikke yderligere fortolkningsbidrag til artikel 7, stk. 1, idet ordlyden i stk. 1 blot fremhæves.

Efter en ordlydsfortolkning må bestemmelsen antages at fastslå, at det er den dataansvarlige, som har bevisbyrden for, at den registrerede har givet det fornødne samtykke, idet bestemmelsen netop nævner, at den dataansvarlige skal kunne "påvise".

Artikel 29-gruppen har i forbindelse med en udtalelse om samtykke anbefalet, at de dataansvarlige inden for rammerne af en generel ansvarlighedsforpligtelse skal kunne bevise, at der er opnået samtykke. Når de dataansvarliges bevisbyrde styrkes, således at det kræves, at de beviser, at de rent faktisk har opnået den registreredes samtykke, vil de være tvunget til at indføre standardmetoder og – mekanismer, der gør, at de kan indhente og bevise, at der er tale om et utvetydigt samtykke. Typen af mekanismer vil afhænge af sammenhængen og bør tage hensyn til forhold og omstændigheder ved behandlingen og ganske særlige risici, der er forbundet med denne.[216]

En sådan bevisbyrde følger allerede af gældende ret, se afsnittet ovenfor. På denne baggrund ses der således med artikel 7, stk. 1, umiddelbart ikke at være tale om en ændring af gældende ret.

Det skal bemærkes, at det med forordningens artikel 7, stk. 1, ikke kan antages, at der indføres et krav om, at samtykket skal afgives skriftligt, idet der blot gælder et krav om, at den dataansvarlige skal kunne påvise samtykket.

Det faktum, at der i forordningen nu er blevet indsat en klar bestemmelse, hvoraf det eksplicit fremgår, at det er den dataansvarlige, som skal kunne påvise, at den registrerede har givet samtykke, er med til at fremhæve betydningen af bevisbyrden. Indsættelsen af en eksplicit bestemmelse taler for, at bevisbedømmelsen skal tillægges større betydning i forbindelse med databehandling fremover. Efter gældende dansk ret er det allerede et krav, at den dataansvarlige skal være i stand til at bevise, at der er afgivet det fornødne samtykke, hvorfor der formelt set ikke sker en ændring i kravene til den dataansvarlige.

3.5.3.2. Databeskyttelsesforordningens artikel 7, stk. 2

Det fremgår af forordningens artikel 7, stk. 2, at hvis den registreredes samtykke gives i en skriftlig erklæring, der også vedrører andre forhold, skal en anmodning om samtykke forelægges på en måde, som klart kan skelnes fra de andre forhold, i en letforståelig og lettilgængelig form og i et klart og enkelt sprog. Enhver del af en sådan erklæring, som udgør en overtrædelse af denne forordning, er ikke bindende.

[216] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s. 40.

Det fremgår af præambelbetragtning nr. 42, at navnlig i forbindelse med skriftlige erklæringer om andre forhold bør garantier sikre, at den registrerede er bekendt med, at og i hvilket omfang der er givet samtykke. I overensstemmelse med Rådets direktiv 93/13/EØF om urimelige kontraktvilkår i forbrugeraftaler bør der stilles en samtykkeerklæring udformet af den dataansvarlige til rådighed i en letforståelig og lettilgængelig form og i et klart og enkelt sprog, og den bør ikke indeholde urimelige vilkår. For at sikre, at samtykket er informeret, bør den registrerede som minimum være bekendt med den dataansvarliges identitet og formålene med den behandling, som personoplysningerne skal bruges til.

Det fremgår således særligt, at ved indhentelse af samtykke på en skriftlig erklæring, som også vedrører andre forhold end samtykke, skal det være klart for den samtykkegivende person, at erklæringen vedrører samtykke.

Som tidligere anført har Artikel 29-gruppen i forbindelse med gældende ret efter databeskyttelsesdirektivet udtalt, at de informationer, der meddeles de registrerede, skal være klare og tilstrækkeligt synlige, så de registrerede ikke overser dem. På denne baggrund må der allerede efter gældende ret ses at være et krav om, at informationer i forbindelse med samtykke skal være tilstrækkeligt synlige. Der er ikke en direkte bestemmelse i gældende ret, som svarer til forordningens artikel 7, stk. 2, 1. pkt. Med forordningen sker der således en præcisering og tydeliggørelse af, at der er et krav om, at informationer omkring samtykke i en skriftlig erklæring skal kunne skelnes fra andre forhold. Der vil kun i mindre omfang være tale om en ændret retstilstand, idet det efter en konkret vurdering allerede i dag antages at ville blive resultatet efter gældende ret, idet et samtykke i dag ikke vil kunne anses som gyldigt afgivet, såfremt der ikke er tale om et informeret samtykke.

Endelig vil der med ordlyden i artikel 7, stk. 2, sidste pkt., om at *"[…] Enhver del af en sådan erklæring, som udgør en overtrædelse af denne forordning, er ikke bindende",* ikke være tale om en ændret retstilstand. Det må således antages at være udtryk for en tydeliggørelse af gældende ret, idet man heller ikke i dag vil kunne bruge et ikke gyldigt samtykke som behandlingshjemmel.

3.5.3.3. Databeskyttelsesforordningens artikel 7, stk. 3

Det følger af forordningens artikel 7, stk. 3, at den registrerede til enhver tid har ret til at trække sit samtykke tilbage. Tilbagetrækning af samtykke berører ikke lovligheden af den behandling, der er baseret på samtykke inden tilbagetrækningen. Inden der gives samtykke, skal den registrerede oplyses om, at samtykket kan trækkes tilbage. Det skal være lige så let at trække sit samtykke tilbage som at give det.

For så vidt angår forordningens artikel 7, stk. 3, 1. og 2. pkt., ses der at være tale om en videreførelse af gældende dansk ret. At der bliver indsat en konkret bestemmelse herom, er derfor en kodificering af retstilstanden på dette område.

Af forordningens artikel 7, stk. 3, 3. pkt., fremgår det, at den registrerede inden samtykket gives skal oplyses om, at samtykket kan trækkes tilbage. Oplysning om, at samtykket kan trækkes tilbage er således nu en gyldighedsbetingelse for det afgivne samtykke. I gældende ret er der som nævnt ovenfor ikke et eksplicit krav om en sådan oplysningspligt i forbindelse med afgivelse af samtykke.

Endvidere indeholder forordningens artikel 7, stk. 3, 4. pkt., et krav om, at det skal være lige så let at trække sit samtykke tilbage, som at give det. I gældende ret ses der, som nævnt ovenfor, ikke at være et direkte krav om, at det skal være lige så let at trække sit samtykke tilbage som at give det.

Det fremgår uddybende af præambelbetragtning nr. 42, at samtykke ikke bør anses for at være frivilligt givet, hvis den registrerede ikke kan tilbagetrække sit samtykke, uden at det er til skade for den pågældende.

Såfremt den registrerede trækker sit samtykke tilbage, er det i den forbindelse vigtigt at holde sig for øje, at der godt kan være flere behandlingshjemler samtidig. Hvis et samtykke trækkes tilbage, *og* der oprindeligt også var hjemmel til behandlingen eksempelvis af hensyn til en legitim interesse, jf. forordningens artikel 6, stk. 1, litra f, vil behandlingen kunne fortsætte efter denne hjemmel.

Endvidere vil en behandling også kunne fortsætte, hvis samtykket trækkes tilbage, såfremt der efterfølgende er mulighed for at benytte en anden behandlingshjemmel.

Hvis den dataansvarlige fortsætter behandlingen, selvom samtykket er trukket tilbage, skal den dataansvarlige være særligt opmærksom på, om den fortsatte behandling vil være i overensstemmelse med princippet om god skik i forordningens artikel 5, stk. 1, litra a.[217]

Forordningens artikel 17, stk. 1, litra b, hvoraf det fremgår, at den registrerede har ret til og den dataansvarlige pligt til at få personoplysninger om sig selv slettet af den dataansvarlige, hvis den registrerede trækker det samtykke, der er grundlaget for behandlingen, jf. artikel 6, stk. 1, litra a, eller artikel 9, stk. 2, litra a, tilbage, *og der ikke er et andet retsgrund-*

[217] Peter Blume, Den nye persondataret (2016), s. 78.

lag for behandlingen, indikerer ligeledes, at der er mulighed for at anvende et andet retsgrundlag, såfremt et samtykke trækkes tilbage.

Da det følger af forordningens artikel 13, stk. 1, litra c, og artikel 14, stk. 1, litra c, at den registrerede skal have oplysning om retsgrundlaget for behandlingen, må den dataansvarlige dog skulle oplyse en registreret – som har trukket sit samtykke tilbage – om, at behandlingen i givet fald fortsætter på baggrund af et andet retsgrundlag.

3.5.3.4. Databeskyttelsesforordningens artikel 7, stk. 4.
Det følger af forordningens artikel 7, stk. 4, at ved vurdering af, om samtykke er givet frit, tages der *størst muligt hensyn* til, *bl.a.* om opfyldelse af en kontrakt, herunder om en tjenesteydelse, er gjort betinget af samtykke til behandling af personoplysninger, *som ikke er nødvendig* for opfyldelse af denne kontrakt.

Bestemmelsen i artikel 7, stk. 4, må antages at være en uddybning af, hvad der skal tages hensyn til i forbindelse med vurderingen af, om et samtykke er afgivet frivilligt efter artikel 4, nr. 11, i forordningen og dermed er gyldigt.

Det fremgår i den forbindelse af præambelbetragtning nr. 43, at samtykke ikke formodes at være givet frivilligt, hvis der er en *klar skævhed* mellem den registrerede og den dataansvarlige, navnlig hvis den dataansvarlige er en offentlig myndighed, og det derfor er usandsynligt, at samtykket er givet frivilligt *under hensyntagen til alle de omstændigheder, der kendetegner den specifikke situation*. Samtykke formodes ikke at være givet frivilligt, hvis det ikke er muligt at give særskilt samtykke til forskellige behandlingsaktiviteter vedrørende personoplysninger, selv om det er hensigtsmæssigt i det enkelte tilfælde, eller hvis opfyldelsen af en kontrakt, herunder ydelsen af en tjeneste, gøres afhængig af samtykke, selv om et sådant samtykke ikke er nødvendigt for dennes opfyldelse.

Det fremhæves således særligt i præambelbetragtning nr. 43, at forordningens artikel 7, stk. 4, også gælder for offentlige myndigheder.

Det fremgår endvidere af præambelbetragtning nr. 42, vedrørende frivillighed, at samtykke ikke bør anses for at være givet frivilligt, hvis den registrerede ikke har et reelt eller frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende.

Netop det faktum, at artikel 7, stk. 4, indeholder ordet *bl.a.* vil bevirke, at bestemmelsen i praksis vil kunne få betydning i en række forskellige situationer, hvor der kan siges at være en klar skævhed mellem den registrerede og den dataansvarlige. Det er vanskeligt at fast-

lægge rækkevidden af denne bestemmelse på forhånd, og bestemmelsen vil utvivlsomt blive udviklet gennem praksis i de kommende år.

Det fremgår som nævnt af artikel 7, stk. 4, at der skal tages størst muligt hensyn. Der ses derfor ikke at være tale om en absolut bestemmelse, som ikke vil kunne fraviges. Bestemmelsen må fastlægge et fortolkningsprincip om størst mulig hensyntagen til "skævheder" ved vurderingen af samtykkets gyldighed.

Forholdet til kontrakter generelt, herunder tjenesteydelser
Det fremgår direkte af forordningens artikel 7, stk. 4, at der skal tages størst muligt hensyn til, om opfyldelse af en kontrakt er gjort betinget af et samtykke til behandling af personoplysninger, som ikke er nødvendig for kontrakten.

Med denne bestemmelse fremgår det, at det skal tillægges størst mulig betydning i vurderingen af, om et samtykke er afgivet frivilligt, hvis en kontrakt betinger et samtykke til behandling af personoplysninger, selvom det efter kontrakten ikke er nødvendigt at behandle personoplysninger.

Såfremt en person ønsker at købe en ydelse fra en virksomhed, vil der således i vurderingen af frivillighed af et eventuelt samtykke skulle tages størst mulig hensyn til, om samtykket eller omfanget heraf til behandling af personoplysninger har været nødvendigt for opfyldelsen af kontrakten.

Dette forhold ses ikke nødvendigvis at være helt i overensstemmelse med gældende ret, idet et samtykke, som anført ovenfor, efter gældende ret generelt må anses for frivilligt, selv om det er afgivet af den registrerede som følge af, at den dataansvarlige ellers ikke har villet indgå i et kontraktforhold med den pågældende. Det må dog formodes, at nogle af de tilfælde, som bestemmelsen rammer, også efter gældende ret vil kunne fanges af kravene om proportionalitet og nødvendighed i persondatalovens § 5.

Med indførelsen af bestemmelsen i artikel 7, stk. 4, vil der nu i sådanne tilfælde under alle omstændigheder ved vurderingen af samtykkets frivillighed skulle tages størst muligt hensyn til, om behandlingen af personoplysningerne er *nødvendig* for opfyldelsen af kontrakten.

Efter forordningens artikel 6, stk. 2, litra b, om almindelige personoplysninger, vil en behandling i forvejen være lovlig, hvis behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.

Under alle omstændigheder er det med artikel 7, stk. 4, slået fast, at der ved vurderingen af om et samtykke er givet frit skal tages størst muligt hensyn til, hvad der er nødvendigt for opfyldelse af kontrakten.

Forholdet til offentlige myndigheder
Præambelbetragtning nr. 43 nævner som anført, at samtykke ikke bør udgøre et gyldigt retsgrundlag for behandlingen, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige, navnlig hvis den dataansvarlige er en offentlig myndighed.

I Kommissionens oprindelige forslag fra 2012 til forordningen fremgik det direkte af forordningens artikel 7, stk. 4, at samtykke ikke tilvejebringer et retsgrundlag for behandling, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige.[218]

I vurderingen af et samtykkes frivillighed skal der som anført tages størst muligt hensyn til, om samtykket er afgivet af en registreret overfor en offentlig myndighed, hvor der er en klar skævhed mellem den registrerede og myndigheden. Dette må eksempelvis antages at kunne være de tilfælde, hvor den registrerede ønsker at ansøge om en ydelse fra en offentlig myndighed, idet der netop i sådanne tilfælde, må antages at være en klar skævhed. Præambelbetragtning nr. 43 vedrører således særligt den situation, hvor en borger har en ret til eksempelvis en ydelse.

Når offentlige myndigheder behandler personoplysninger med hjemmel i forordningens artikel 6, stk. 1, litra a, og artikel 9, stk. 2, litra a, bør samtykket efter præambelbetragtning nr. 43, sammenholdt med artikel 7, stk. 4, ikke udgøre et gyldigt retsgrundlag for behandlingen, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige.

Bestemmelsen ses ud fra en ordlydsfortolkning af artikel 7, stk. 4, (”som ikke er nødvendig”) dog ikke at føre til, at samtykke ikke kan benyttes som hjemmel i sådanne tilfælde - bestemmelsen forudsætter således ”blot”, at behandlingen af de pågældende oplysninger skal være nødvendig for opfyldelsen. I den forbindelse må det forudsættes, at nødvendighedskravet vil være opfyldt, hvis myndigheden har brug for personoplysningerne for at kunne behandle den pågældende registreredes sag. Med udtrykket, at myndigheden *har brug for* personoplysningerne menes, at myndigheden som følge af indretningen af lovgivningen ikke kan indhente de relevante oplysninger på anden måde.

Der kan i den forbindelse henvises til, at det af punkt 199 i vejledning nr. 11740/1986 om forvaltningsloven vedrørende officialmaksimen fremgår, at det er et helt grundlæggende

[218] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig).

princip i dansk forvaltningsret, at det påhviler den enkelte forvaltningsmyndighed selv, eventuelt i samarbejde med andre myndigheder, at fremskaffe fornødne oplysninger om de foreliggende sager eller dog at foranledige, at private, navnlig parterne, yder medvirken til sagens oplysning.

Alternativt vil den offentlige myndighed i tvivlstilfælde kunne overveje andre behandlingshjemler såsom artikel 6, stk. 1, litra e, om bl.a., at behandling kan foretages, hvis den er nødvendig af hensyn til udførelse af en opgave, som henhører under offentlig myndighedsudøvelse eller artikel 9, stk. 1, litra g, om væsentlige samfundsinteresser.

Ansættelsesforhold
Et ansættelsesforhold vil også være et kontraktforhold, hvorfor artikel 7, stk. 4, også vil kunne være relevant i denne forbindelse.

Særligt i forhold til det ansættelsesretlige område, fremgår det bl.a. af forordningens artikel 88, stk. 1, at medlemsstaterne ved lov eller i medfør af kollektive overenskomster kan fastsætte mere specifikke bestemmelser for at sikre beskyttelse af rettighederne og frihedsrettighederne i forbindelse med behandling af arbejdstageres personoplysninger i ansættelsesforhold.

Specifikt vedrørende samtykke i den ansættelsesretlige situation fremgår det endvidere af præambelbetragtning nr. 155 bl.a., at medlemsstaternes nationale ret eller kollektive overenskomster, herunder »lokalaftaler«, kan fastsætte specifikke bestemmelser om behandling af arbejdstageres personoplysninger i ansættelsesforhold, navnlig betingelserne for, hvorledes personoplysninger i ansættelsesforhold kan behandles på grundlag af arbejdstagerens samtykke.

Efter forordningens artikel 88, stk. 1, og præambelbetragtning nr. 155 synes der umiddelbart at være rum for, at det nationalt kan bestemmes, hvorledes samtykke kan benyttes inden for det ansættelsesretlige område. For nærmere herom kan der henvises til afsnit 10.4. om ansættelsesforhold.

3.5.3.5. Overgang
Vedrørende samtykke skal det afslutningsvis bemærkes, at det fremgår af præambelbetragtning nr. 171, at når behandling er baseret på samtykke i henhold til databeskyttelsesdirektivet, er det ikke nødvendigt, at den registrerede på ny giver sit samtykke, når forordningen skal anvendes, såfremt den måde, som samtykket er givet på, er i overensstemmelse med betingelserne i denne forordning; i så fald kan den dataansvarlige fortsætte behandlingen efter forordningens anvendelsesdato, jf. artikel 94, stk. 1.

Det nye krav om, at den registrerede inden samtykket gives skal oplyses om, at samtykket kan trækkes tilbage, jf. forordningens artikel 7, stk. 3, 3. pkt., er som tidligere nævnt en gyldighedsbetingelse for det afgivne samtykke.

Dette nye krav finder dog først anvendelse fra den 25. maj 2018, hvorfra forordningen i øvrigt finder anvendelse. EU-lovgiver kan således ikke have haft en forventning om, at et tidligere indhentet samtykke er indhentet med en samtidig oplysning om, at det kan trækkes tilbage. Oplysningen om tilbagetrækningsmuligheden kan således ikke antages at være en ny gyldighedsbetingelse for et eksisterende samtykke. Andet ville gøre præambelbetragtning nr. 171 om muligheden for at behandle videre på baggrund af et eksisterende samtykke indholdsløs.

Det bemærkes, at det kan være en god idé – hvis det er praktisk muligt – før den 25. maj 2018 at oplyse den registrerede om, at samtykket kan trækkes tilbage. Det bemærkes i den forbindelse, at et samtykke efter gældende ret i persondatalovens § 38 kan trækkes tilbage, jf. nærmere ovenfor.

Et samtykke, der forud for den 25. maj 2018 er indhentet i overensstemmelse med de gældende regler herom, må på den baggrund antages også at kunne anvendes som hjemmel fra og med den dato.

3.5.4. Overvejelser

Vedrørende artikel 7, stk. 1, om bevisbyrden for et gyldigt samtykke, vil indsættelsen af en eksplicit bestemmelse om, at det er den dataansvarlige, som skal kunne påvise, at den registrerede har givet samtykke, tale for, at bevisbedømmelsen tillægges større betydning i forbindelse med behandling fremover. Efter gældende dansk ret er det allerede et krav, at den dataansvarlige skal være i stand til at vise, at der er afgivet det fornødne samtykke, hvorfor der formelt set dog ikke sker en ændring i kravene til den dataansvarlige.

Vedrørende artikel 7, stk. 2, og stk. 3, 1. og 2. pkt., om informeret samtykke og tilbagetrækning af samtykke, vil der ikke være tale om en ændring i forhold til gældende ret, idet retstilstanden ses at være i overensstemmelse hermed.

For så vidt angår artikel 7, stk. 3, 3. og 4. pkt., om oplysning om tilbagetrækning af samtykke, er der tale om nyaffattede krav til samtykke for den dataansvarlige og oplysningen om, at samtykket kan trækkes tilbage er tilmed en gyldighedsbetingelse for det afgivne samtykke. Det ses således ikke ud fra praksis i gældende dansk ret at være blevet fastslået, at der helt generelt gælder sådanne krav. Det kan dog ikke udelukkes, at denne retstilstand ville kunne blive resultatet i en konkret sag efter gældende ret. Ikke desto mindre, så fast-

lægger forordningen klart disse krav til samtykke, hvorfor de dataansvarlige i hvert fald, når forordningen finder anvendelse fra den 25. maj 2018, vil skulle overholde kravene heri.

Med indsættelsen af artikel 7, stk. 4, om frivilligt samtykke, er der overordnet tale om en ændring af gældende ret.

3.6. Børns samtykke i forbindelse med informationssamfundstjenester, artikel 8

3.6.1. Præsentation

I gældende ret er der ikke en bestemmelse, som direkte regulerer betingelserne for børns samtykke i forbindelse med informationssamfundstjenester.

Reglerne omkring børns samtykke følger af de generelle betingelser i persondataloven til et samtykkes gyldighed.

3.6.2. Gældende ret

I Danmark er børn og unge under 18 år, der ikke har indgået ægteskab, mindreårige og dermed umyndige.[219]

I gældende ret er der ikke fastsat direkte regler for, hvornår et samtykke fra et barn efter persondataloven vil være gyldigt. Reglerne vedrørende betingelser for et barns samtykke i forbindelse med informationssamfundstjenester følger således af persondatalovens generelle regler om samtykke.

Af relevans herfor fremgår det af rettighedsvejledningen[220] til persondataloven, pkt. 3.1.4 om indsigt i oplysninger om børn og unge under 18 år, at persondataloven bygger på et individuelt modenhedskriterium, jf. nærmere herom nedenfor.

Datatilsynet har i årsberetning fra 2003 udtalt, at tilsynet i en konkret sag umiddelbart vurderede, at et barn, der er i stand til selv at logge sig på et chatrum og dér afgive oplysninger, som udgangspunkt normalt også gyldigt vil kunne samtykke til den omhandlede databehandling. Datatilsynet lagde i denne forbindelse især vægt på, at barnet selv aktivt skal logge sig på chatrummet, at barnet selv skriver og dermed afgiver de omhandlede oplys-

[219] § 1 i værgemålsloven, jf. lovbekendtgørelse nr. 1015 af 20. august 2007 med senere ændringer.
[220] Vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger

ninger, og at oplysningerne efter det oplyste i øvrigt ikke ville blive lagret og senere anvendt til andre formål.[221]

I en sag om behandling af personoplysninger vedrørende lagring af chat hos Jubii har Datatilsynet tilsvarende udtalt, at et barn, der er i stand til at logge sig på et chatrum, og dér afgive oplysninger, som udgangspunkt normalt også gyldigt vil kunne samtykke til den omhandlede databehandling. Datatilsynet understregede dog i sagen, at afgørelsen af, hvorvidt der foreligger et gyldigt samtykke, beror på en konkret vurdering i hver enkelt situation, hvor bl.a. barnets individuelle modenhed har betydning.[222]

Spørgsmålet om, hvorvidt mindreårige på egen hånd kan meddele samtykke til behandling af personoplysninger, er vedrørende den offentlige forvaltning behandlet i forvaltningsloven med kommentarer, hvor det vedrørende forvaltningslovens § 29 om indhentning af følsomme personoplysninger i ansøgningssager anføres, at hvis den mindreårige på egen hånd kan indgive ansøgning til en forvaltningsmyndighed, må den pågældende derfor også selv kunne meddele samtykke til de fornødne forvaltningsprocessuelle skridt, herunder til indsamling og videregivelse af personoplysninger. Det fremgår endvidere, at hvis lovgivningen ikke indeholder regler eller forudsætninger om, at den mindreårige kan optræde på egen hånd, må det antages, at den mindreårige selv kan meddele samtykke, hvis den unge har den modenhed, som på det givne sagsområde er nødvendigt for at forstå og overse konsekvenserne af samtykket, og der er grund til at antage, at der foreligger stiltiende samtykke fra forældremyndighedsindehaveren, eller at denne ikke vil modsætte sig samtykket.[223]

Endelig er der blandt andet i sundhedsloven regler om, at en patient, der er fyldt 15 år, kan give samtykke til videregivelse af helbredsoplysninger.

Artikel 29-gruppen udtaler vedrørende samtykke, at børn bør behandles i overensstemmelse med deres fysiske og psykiske modenhed, og at de fra og med en vis alder er i stand til at tage stilling til spørgsmål, som vedrører dem.[224]

Artikel 29-gruppen anfører, at alderen for, hvornår samtykke kan opnås fra et barn varierer, og at der ikke er nogen harmonisering for, hvordan man verificerer et barns alder. I den forbindelse anfører Artikel 29-gruppen, at de finder, at børns interesse ville blive tilgodeset bedre, hvis databeskyttelsesreglerne indeholdt bestemmelser herom.[225]

[221] Datatilsynets årsberetning for 2003, s. 141.
[222] Sag om lagring af chat hos Jubii, Datatilsynets j.nr. 2002-219-0136.
[223] Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave, 2013, s. 832.
[224] Artikel 29-grupppens udtalelse nr. 2/2009 om beskyttelse af børns personoplysninger (WP 160), s.6-9.
[225] Artikel 29-gruppens udtalelse nr. 15/2011 om definitionen af samtykke (WP 187), s. 28.

Vedrørende forældremyndighedsindehaverens samtykke på vegne af barnet, antages det, at forældre til mindreårige børn i almindelighed kan give samtykke på vegne af deres børn, idet det dog konkret må vurderes, om dette i forhold til bl.a. oplysningernes karakter bør accepteres.[226]

Efter en samlet vurdering er retstilstanden efter gældende ret i forhold til børns afgivelse af samtykke, at afgørelsen af, hvorvidt der foreligger et gyldigt samtykke, beror på en konkret vurdering i hver enkelt situation, hvor bl.a. barnets individuelle modenhed har betydning. Endvidere ses der i gældende ret ikke at være særlige regler for afgivelse af børns samtykke i forbindelse med informationssamfundstjenester.

3.6.3. Databeskyttelsesforordningen

Artikel 8 i forordningen indeholder nye regler for et barns samtykke i forbindelse med informationssamfundstjenester.

Det fremgår af artikel 8, stk. 1, at hvis artikel 6, stk. 1, litra a, finder anvendelse i forbindelse med udbud af *informationssamfundstjenester* direkte til børn, er behandling af personoplysninger om et barn lovlig, hvis barnet er mindst 16 år. Er barnet under 16 år, er sådan behandling kun lovlig, hvis og i det omfang samtykke gives eller godkendes af indehaveren af forældremyndigheden over barnet. Medlemsstaterne kan ved lov fastsætte en lavere aldersgrænse til disse formål, forudsat at en sådan aldersgrænse ikke er under 13 år.

Det fremgår af forordningens artikel 6, stk. 1, litra a, at behandling af "almindelige" personoplysninger er lovlig, hvis den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.

I forordningens artikel 4, nr. 25, er informationssamfundstjeneste defineret som en tjeneste som defineret i artikel 1, stk. 1, litra b, i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 (informationsproceduredirektivet).

Af dette direktivs artikel 1, stk. 1, litra b, fremgår, at der ved begrebet "tjeneste" forstås enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager.

Af eksempler, som er omfattet af informationsproceduredirektivet, har Kommissionen før nævnt onlineinformationstjenester af generel karakter (såsom aviser, databaser osv.), tele-

[226] Persondataloven med kommentarer (2015), s. 168.

overvågningsaktiviteter, interaktivt teleindkøb, elektronisk post, onlinereservation af flybilletter, professionelle onlinetjenesteydelser (adgang til databaser, diagnosticering osv.).

Umiddelbart antages det, at offentlige selvbetjeningsløsninger og andre offentlige onlinetjenester, som eksempelvis NemID, ikke betragtes som en tjeneste, der betales en økonomisk modydelse for at bruge, hvorfor sådanne løsninger som udgangspunkt ikke er omfattet af begrebet "informationssamfundstjeneste".

Det fremgår endvidere af præambelbetragtning nr. 38, at børn bør nyde særlig beskyttelse af deres personoplysninger, eftersom de ofte er mindre bevidste om de pågældende risici, konsekvenser og garantier og deres rettigheder for så vidt angår behandling af personoplysninger. En sådan særlig beskyttelse bør navnlig gælde for brug af børns personoplysninger med henblik på markedsføring eller til at oprette personligheds- eller brugerprofiler og indsamling af personoplysninger vedrørende børn, når de anvender tjenester, der tilbydes direkte til et barn.

Artikel 8, stk. 1, om *informationssamfundstjenester direkte til børn* må således også antages at kunne omfatte eksempelvis Facebook, Instagram og Snapchat.

Det fremgår endvidere af præambelbetragtning nr. 38, at samtykke fra indehaveren af forældremyndigheden ikke er nødvendig – underforstået heller ikke for børn under den angivne aldersgrænse – når det drejer sig om forebyggende eller rådgivende tjenester, der tilbydes direkte til et barn. Denne betragtning fører til, at eksempelvis tjenester som BørneTelefonen ikke vil være omfattet af alderskravet for samtykke. Det samme gør sig gældende for andre private og offentlige rådgivende tilbud til børn og unge. Dette stemmer også overens med, at forebyggende og rådgivende tjenester til børn netop er tjenester, som barnet kan have brug for at kunne tilgå, uden at forældremyndighedsindehaveren er vidende herom eller samtykker heri.

Det fremgår af artikel 8, stk. 2, at under hensyntagen til den tilgængelige teknologi skal den dataansvarlige gøre sig rimelige bestræbelser på i sådanne tilfælde at kontrollere, at indehaveren af forældremyndigheden over barnet har givet eller godkendt samtykket.

Kravene til den dataansvarliges bestræbelser må i den forbindelse forventes nærmere at blive præciseret ved adfærdskodekser. Det fremgår således af forordningens artikel 40, stk. 2, litra g, at sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, kan udarbejde adfærdskodekser eller ændre eller udvide sådanne kodekser med henblik på at specificere den information, der gives til børn, beskyt-

telsen af børn og den måde, hvorpå samtykket fra indehavere af forældremyndighed over børn skal indhentes.

Det følger endelig af artikel 8, stk. 3, at stk. 1 ikke berører medlemsstaternes generelle aftaleret, som f.eks. bestemmelser om gyldighed, indgåelse eller virkning af en kontrakt, når der er tale om et barn.

3.6.4. Overvejelser

Med artikel 8 sker der en ændring i forhold til gældende ret, idet der nu bliver fastsat en aldersgrænse for, hvornår et samtykke fra et barn er gyldigt i forbindelse med informationssamfundstjenester. Der indføres endvidere et krav om samtykke eller godkendelse af samtykke fra forældremyndighedsindehaveren, såfremt barnet er under den fastsatte alder. Endelig fremhæves det, at den dataansvarlige skal gøre sig rimelige bestræbelser på at kontrollere, at forældremyndighedsindehaveren har givet eller godkendt samtykket.

I artikel 8, stk. 1, efterlades medlemsstaterne en mulighed for ved lov at fastsætte en lavere aldersgrænse end 16 år, dog ikke under 13 år.

3.7. Følsomme oplysninger, artikel 9, stk. 1

3.7.1. Præsentation

Databeskyttelsesforordningens artikel 9 indeholder en særlig kategori af personoplysninger, som er følsomme.

3.7.2. Gældende ret

Det fremgår af persondatalovens § 7, stk. 1, at der ikke må behandles oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

Bestemmelsen bygger på artikel 8, stk. 1, i databeskyttelsesdirektivet. Det fremgår af forarbejderne til persondatalovens § 7, stk. 1, at opregningen af typer af følsomme personoplysninger er udtømmende.[227] Persondatalovens § 7, stk. 1, omfatter således kun de typer af følsomme personoplysninger, som er nævnt i databeskyttelsesdirektivets artikel 8, stk. 1.

[227] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.

Omfattet af udtrykket *helbredsmæssige forhold* er oplysninger om en fysisk persons tidligere, nuværende og fremtidige fysiske eller psykiske tilstand samt oplysninger om medicinmisbrug og misbrug af narkotika, alkohol og lignende nydelsesmidler.[228]

Højesteret udtalte i dom U 2011.2343 H, at en oplysning om alkoholmisbrug eller mistanke herom er omfattet af begrebet *helbredsmæssige forhold*. I sagen videregav en medarbejder i en kommune til en medarbejder i en anden kommune oplysning om, at der var mistanke om alkoholmisbrug hos en tidligere medarbejder i kommunen, som nu søgte job i den anden kommune. Højesteret fandt, at denne videregivelse var omfattet af persondatalovens § 7, stk. 1.

I sag C-101/01, Lindqvist, dom af 6. november 2003, havde en person oprettet hjemmesider på internettet for at gøre det let for medlemmerne af menigheden at forberede konfirmation. I den forbindelse havde personen på en hjemmeside oplyst, at personens kollega havde beskadiget foden og var delvist sygemeldt. EU-Domstolen udtalte i den forbindelse, at der bør anlægges en vid fortolkning af udtrykket *oplysninger om helbredsforhold* i artikel 8, stk. 1, således at det omfatter oplysninger vedrørende alle aspekter, såvel fysiske som psykiske af en persons helbred. EU-Domstolen fastslog, at en oplysning om, at en person har beskadiget sin fod og er delvist sygemeldt, udgør en helbredsoplysning.

Oplysning om, at en person er syg, uden angivelse af, hvori sygdommen består, kan dog ikke anses for en helbredsoplysning.[229]

I den forbindelse har Østre Landsret i dom af 17. april 2008 i sag nr. B-653-07 udtalt, at en oplysning om, at en medarbejder havde været langtidssygemeldt (uden nogen nærmere angivelse af baggrunden herfor) var omfattet af persondatalovens § 6, stk. 1.

Fagforeningsmæssige forhold omfatter utvivlsomt oplysning om, at en person er medlem af en bestemt fagforening, mens en oplysning om manglende medlemskab ikke kan antages at være omfattet af § 7, stk. 1.[230]

Endelig vil personoplysninger også kunne være omfattet af persondatalovens § 7, stk. 1, selv om oplysningstypen ikke er nævnt direkte, hvis følsomme oplysninger kan udledes af den sammenhæng, hvori den pågældende person er omtalt. Dette vil eksempelvis kunne

[228] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[229] Persondataloven med kommentarer (2015), s. 284.
[230] Persondataloven med kommentarer (2015), s. 283.

være en adresseoplysning, som afslører noget om, at en person f.eks. har bopæl på et psykiatrisk hospital.

Datatilsynet anser normalt ikke oplysninger om nationalitet eller navn for at være omfattet af persondatalovens § 7, stk. 1, selvom sådanne oplysninger undertiden kan give en mere eller mindre kraftig indikation af eksempelvis etnisk baggrund eller religiøs overbevisning.[231]

Biometriske oplysninger
Artikel 29-gruppen har udtalt, at behandlingen af biometriske oplysninger skal være baseret på et af de legitime grundlag, som er beskrevet i artikel 7 i databeskyttelsesdirektivet[232] – som svarer til persondatalovens § 6. Som tidligere anført vil den sammenhæng, som oplysningen indgår i, kunne bevirke, at den vil være omfattet af persondatalovens § 7, stk. 1. Det samme vil være tilfældet ved biometriske oplysninger, såfremt disse eksempelvis afslører racemæssig eller etnisk baggrund eller oplysninger om en persons helbredstilstand.[233]

Datatilsynet anser efter praksis biometriske oplysninger som omfattet af persondatalovens § 6. Som eksempel kan nævnes en sag vedrørende adgangskontrol ved brug af ansigtsgenkendelse, hvor tilsynet udtalte, at løsningen efter det oplyste kun benytter afstanden mellem øjnene samt ansigtets form som identifikation. Andre personlige træk såsom race er ikke parametre, der anvendes i systemet. Efter Datatilsynets opfattelse var der tale om behandling af almindelige ikke-følsomme oplysninger omfattet af persondatalovens § 6.[234]

Endvidere udtalte Datatilsynet i en sag vedrørende brug af fingeraftryk ved tidsregistrering af aktiverede borgere, at behandling af biometriske oplysninger som udgangspunkt skal vurderes i forhold til persondatalovens § 6, stk. 1, der regulerer behandling af almindelige ikke-følsomme oplysninger.[235]

3.7.3. Databeskyttelsesforordningen
Det fremgår af databeskyttelsesforordningens artikel 9, stk. 1, at behandling af personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske

[231] Persondataloven med kommentarer (2015), s. 287.
[232] Artikel 29-gruppens udtalelse 3/2012 om udviklingen inden for biometriske teknologier, (WP 193) s. 10.
[233] Artikel 29-gruppens udtalelse 3/2012 om udviklingen inden for biometriske teknologier, (WP 193) s. 15.
[234] Udtalelse om adgangskontrol ved brug af ansigtsgenkendelse, Datatilsynets j.nr. 2009-082-0087.
[235] Udtalelse om tidsregistrering af aktiverede borgere ved brug af fingeraftryk, Datatilsynets j.nr. 2010-323-0140.

data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt.

Det fremgår endvidere af præambelbetragtning nr. 51, at personoplysninger, der i kraft af deres karakter er særligt følsomme i forhold til grundlæggende rettigheder og frihedsrettigheder, bør nyde specifik beskyttelse, da sammenhængen for behandling af dem kan indebære betydelige risici for grundlæggende rettigheder og frihedsrettigheder. Det fremgår endvidere af betragtningen, at disse personoplysninger bør omfatte personoplysninger om race eller etnisk oprindelse, idet anvendelsen af udtrykket »race« i denne forordning ikke betyder, at Unionen accepterer teorier, der søger at fastslå, at der findes forskellige menneskeracer. Endelig fremgår det af betragtningen, at behandling af fotografier ikke systematisk bør anses for at være behandling af særlige kategorier af personoplysninger, eftersom de kun vil være omfattet af definitionen af biometriske data, når de behandles ved en specifik teknisk fremgangsmåde, der muliggør entydig identifikation eller autentifikation af en fysisk person.

Det fremgår af databeskyttelsesforordningens artikel 4, stk. 15, at "helbredsoplysninger" i forordningen forstås ved personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand.

Det fremgår endvidere af præambelbetragtning nr. 35, at helbredsoplysninger bør omfatte alle personoplysninger om den registreredes helbredstilstand, som giver oplysninger om den registreredes tidligere, nuværende eller fremtidige fysiske eller mentale helbredstilstand. Dette omfatter oplysninger om den fysiske person indsamlet i løbet af registreringen af denne med henblik på eller under levering af sundhedsydelser, jf. Europa-Parlamentets og Rådets direktiv 2011/24/EU (9), til den fysiske person; et nummer, symbol eller særligt mærke, der tildeles en fysisk person for entydigt at identificere den fysiske person til sundhedsformål; oplysninger, der hidrører fra prøver eller undersøgelser af en legemsdel eller legemlig substans, herunder fra genetiske data og biologiske prøver; og enhver oplysning om f.eks. en sygdom, et handicap, en sygdomsrisiko, en sygehistorie, en sundhedsfaglig behandling eller den registreredes fysiologiske eller biomedicinske tilstand uafhængigt af kilden hertil, f.eks. fra en læge eller anden sundhedsperson, et hospital, medicinsk udstyr eller in vitro-diagnostik.

Bestemmelsen i forordningens artikel 9, stk. 1, svarer efter ordlyden stort set til bestemmelsen i databeskyttelsesdirektivets artikel 8, stk. 1. Databeskyttelsesdirektivets artikel 8, stk. 1, er implementeret ved persondatalovens § 7, stk. 1, og derfor udtryk for gældende

ret. På denne baggrund ses det således umiddelbart ikke at være hensigten med databeskyttelsesforordningens artikel 9, stk. 1, at der skal ske en ændring af gældende ret.

Databeskyttelsesforordningens artikel 9, stk. 1, indeholder dog en sproglig tilføjelse i forhold til, at bestemmelsen nævner, at oplysninger om en fysisk persons seksuelle forhold eller *seksuelle orientering* vil være en følsom oplysning.

I databeskyttelsesdirektivets artikel 8, stk. 1, samt i persondatalovens § 7, stk. 1, nævner bestemmelserne kun seksuelle forhold. Selvom der i forordningen yderligere er anført oplysninger om seksuel orientering, må det kunne lægges til grund, at en persons seksuelle orientering også efter gældende ret er omfattet af begrebet "oplysninger om seksuelle forhold". Det ses derfor ikke, at det med denne tilføjelse er hensigten, at der skal ske en ændring af gældende ret.

Det skal endvidere bemærkes, at forordningens artikel 9, stk. 1, også oplister *behandling af genetiske data* samt *biometriske data med det formål entydigt at identificere en fysisk person* som omfattet af bestemmelsen.

Det fremgår af forordningens artikel 4, nr. 13, at »genetiske data« er personoplysninger vedrørende en fysisk persons arvede eller erhvervede genetiske karakteristika, som giver entydig information om den fysiske persons fysiologi eller helbred, og som navnlig foreligger efter en analyse af en biologisk prøve fra den pågældende fysiske person.

Det fremgår endvidere af præambelbetragtning nr. 34, at genetiske data bør defineres som personoplysninger vedrørende en fysisk persons arvede eller erhvervede genetiske karakteristika, som foreligger efter en analyse af en biologisk prøve fra den pågældende fysiske person, navnlig en analyse på kromosomniveau af deoxyribonukleinsyre (DNA) eller af ribonukleinsyre (RNA), eller efter en analyse af et andet element til indhentning af lignende oplysninger.

På baggrund af selve definitionen af genetisk data, vil sådanne oplysninger formentlig oftest have været følsomme oplysninger efter gældende ret, idet de kan karakteriseres som helbredsoplysninger. Med forordningens artikel 9, stk. 1 bliver det i hvert fald præciseret, at sådanne oplysninger nu er omfattet af bestemmelsen.

Det fremgår endvidere af forordningens artikel 4, nr. 14, at »biometriske data« er personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger.

Biometrisk data må skulle forstås i overensstemmelse med udtrykket "biometriske oplysninger" efter gældende ret.

Templates – som er en matematisk udregnet værdi af eksempelvis et fingeraftryk eller et billede – med det formål entydigt at identificere en fysisk person vil, særligt på baggrund af definitionen i artikel 4, stk. 14, også være omfattet af definitionen og derfor omfattet af databeskyttelsesforordningens artikel 9 om følsomme oplysninger. Det bemærkes, at oplysninger om templates efter gældende ret alene behandles som en almindelig oplysning omfattet af persondatalovens § 6.

Som tidligere nævnt bliver biometrisk data med det formål entydigt at identificere en fysisk person ikke anset som følsomme oplysninger efter gældende ret, hvorfor der med forordningen sker en ændring, som bevirker, at sådanne personoplysninger nu er omfattet af kategorien af følsomme oplysninger, jf. forordningens artikel 9, stk. 1.

3.7.4. Overvejelser

Databeskyttelsesforordningens artikel 9, stk. 1, er overordnet set en videreførelse af gældende ret. For så vidt angår biometrisk data med det formål entydigt at identificere en fysisk person bliver dette – modsat efter gældende ret – når forordningen finder anvendelse fra den 25. maj 2018, omfattet af den særlige kategori af personoplysninger i artikel 9, stk. 1, samtidig bliver det hermed præciseret, at genetisk data er følsomme oplysninger.

3.8. Hjemler til behandling af følsomme oplysninger, artikel 9, stk. 2-3

3.8.1. Præsentation

Persondatalovens § 7 vedrører følsomme oplysninger, samt hvornår der kan ske behandling af disse oplysninger.

Databeskyttelsesforordningens artikel 9 indeholder tilsvarende regler for behandling af særlige kategorier af personoplysninger.

Artikel 9, stk. 1, oplister, hvilke personoplysninger, som er særlige kategorier, mens det af artikel 9, stk. 2, fremgår, hvornår behandling af sådanne særlige kategorier af oplysninger kan finde sted.

Endvidere følger det af artikel 9, stk. 3, at personoplysninger, som omhandlet i stk. 1 kan behandles til de formål, der er nævnt i stk. 2, litra h, hvis disse oplysninger behandles af en fagperson, der har tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale

ret eller regler, der er fastsat af nationale kompetente organer, eller under en sådan persons ansvar, eller af en anden person, der også har tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret eller regler, der er fastsat af nationale kompetente organer.

3.8.2. Gældende ret

Behandling af følsomme oplysninger omfattet af persondatalovens § 7 må finde sted, hvis mindst én af betingelserne i § 7 er opfyldt.

Persondatalovens § 7 bygger på artikel 8, stk. 2, i databeskyttelsesdirektivet.

Det fremgår af bemærkningerne til persondataloven, at lovens § 7 fastsætter en række tilfælde, hvor behandling af personoplysninger, som er omfattet af stk. 1, kan finde sted. Bestemmelsen bygger på direktivets artikel 8, stk. 2, som må antages at indeholde en udtømmende opregning af, hvornår behandling af oplysninger som nævnt i artikel 8, stk. 1, kan finde sted.[236]

For de bestemmelser, som har et krav om nødvendighed, vil det bero på den konkrete situation, hvorvidt en given behandling af oplysninger må antages at være nødvendig i bestemmelsens forstand. Med kravet om, at behandlingen skal være nødvendig, er der således overladt et vist skøn til den dataansvarlige. Dette skøn vil dog altid kunne efterprøves af vedkommende tilsynsmyndighed, hvorfor en nærmere fastlæggelse af, hvornår behandling af følsomme oplysninger er nødvendig, derfor må ske gennem tilsynsmyndighedens virksomhed. Vurderingen af behandlingens nødvendighed afhænger af, hvilken form for behandling der er tale om.[237]

3.8.2.1. Persondatalovens § 7, stk. 2, nr. 1 (der svarer til databeskyttelsesforordningens artikel 9, stk. 2, litra a)

Det følger af persondatalovens § 7, stk. 2, nr. 1, at behandling af følsomme oplysninger, må finde sted, hvis den registrerede har givet sit udtrykkelige samtykke hertil.

Denne bestemmelse er baseret på artikel 8, stk. 2, litra a, i databeskyttelsesdirektivet, hvoraf det fremgår, at behandling af følsomme oplysninger må finde sted, hvis den registrerede udtrykkeligt har givet sit samtykke til en sådan behandling, medmindre det i medlemsstatens lovgivning fastsættes, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke. Det fremgår af præambelbetragtning nr. 33 til direktivet, at oplysnin-

[236] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[237] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.

ger, som ifølge deres art kan krænke de grundlæggende frihedsrettigheder eller privatlivets fred, ikke må gøres til genstand for behandling uden den registreredes udtrykkelige samtykke.

Det fremgår endvidere af bemærkningerne til persondataloven, at behandling af oplysninger må finde sted, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Samtykkekravet skal forstås i overensstemmelse med den legale definition i persondatalovens § 3, nr. 8. Der skal således være tale om en frivillig, specifik og informeret viljestilkendegivelse. Et samtykke skal meddeles på en sådan måde, at det klart og utvetydigt fremgår, at den registrerede har meddelt sit samtykke til behandlingen. Herudover skal samtykket være udtrykkeligt. Heraf følger, at den dataansvarlige ikke vil kunne opnå stiltiende eller indirekte tilslutning til behandling af de i stk. 1 nævnte oplysninger. Et egentligt krav om skriftlighed følger ikke af bestemmelsen. Der bør dog i videst muligt omfang søges indhentet et skriftligt samtykke fra den registrerede, idet der herved opnås klarhed omkring samtykkets rækkevidde.[238]

3.8.2.2 Persondatalovens § 7, stk. 3 (der stort set svarer til databeskyttelsesforordningens artikel 9, stk. 2, litra b)

Det fremgår af persondatalovens § 7, stk. 3, at behandling af oplysninger om *fagforeningsmæssige tilhørsforhold* endvidere kan ske, hvis behandlingen er nødvendig for overholdelsen af den dataansvarliges arbejdsretlige forpligtelser eller specifikke rettigheder.

Persondatalovens § 7, stk. 3, er en implementering af databeskyttelsesdirektivets artikel 8, stk. 2, litra b, hvoraf det fremgår, at behandling af følsomme oplysninger må ske, hvis behandlingen er nødvendig for overholdelsen af den dataansvarliges arbejdsretlige forpligtelser og specifikke rettigheder, for så vidt den er tilladt ifølge nationale lovbestemmelser, som fastsætter de fornødne garantier.

Det fremgår af bemærkningerne til persondatalovens § 7, stk. 3, at udtrykket arbejdsretlige forpligtelser eller specifikke rettigheder skal forstås i bred forstand. Omfattet af udtrykket er alle former for forpligtelser og rettigheder, som hviler på et arbejdsretligt grundlag. Dette gælder, uanset om grundlaget er lovgivning eller aftale. Også behandling af oplysninger, som sker til overholdelse af forpligtelser eller rettigheder, som følger af kollektive overenskomster mellem arbejdsmarkedets parter eller af individuelle ansættelseskontrakter, er dermed omfattet af bestemmelsen.[239]

[238] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[239] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.

Det fremgår yderligere om baggrunden for formuleringen af persondatalovens § 7, stk. 3, i betænkning nr. 1345, at Registerudvalget fandt, at den dataansvarliges adgang til at foretage behandling af oplysninger med henblik på at overholde dennes arbejdsretlige forpligtelser eller udøve dennes specifikke arbejdsretlige rettigheder, bør begrænses til oplysninger om enkeltpersoners fagforeningsmæssige forhold.[240]

3.8.2.3. Persondatalovens § 7, stk. 2, nr. 2 (der svarer til databeskyttelsesforordningens artikel 9, stk. 2, litra c)

Det følger af persondatalovens § 7, stk. 2, nr. 2, at behandling af følsomme oplysninger, må finde sted, hvis behandlingen er nødvendig for at beskytte den registreredes eller en anden persons vitale interesser i tilfælde, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke.

Bestemmelsen svarer til artikel 8, stk. 2, litra c, i databeskyttelsesdirektivet.

Det fremgår af bemærkningerne til persondataloven, at bestemmelsen, der skal ses som et supplement til bestemmelsen i nr. 1, bl.a. omfatter den situation, at den registrerede på grund af sygdom eller andre fysisk betingede omstændigheder, som eksempelvis senildemens og bevidstløshed, ikke er i stand til at meddele sit samtykke. Omfattet af bestemmelsen er endvidere den situation, at der foreligger juridiske hindringer for den registreredes meddelelse af samtykke til behandlingen. Dette vil eksempelvis være tilfældet, hvis den registrerede er frataget sin retlige handleevne.[241]

Endvidere fremgår det af bemærkningerne, at for så vidt angår udtrykket vitale interesser, henvises til bemærkningerne til bestemmelsen i § 6, stk. 1, nr. 4.[242]

3.8.2.4. Persondatalovens § 7, stk. 4 (der svarer til databeskyttelsesforordningens artikel 9, stk. 2, litra d)

Det følger af persondatalovens § 7, stk. 4, at en stiftelse, en forening eller en anden almennyttig organisation, hvis sigte er af politisk, filosofisk, religiøs eller faglig art, inden for rammerne af sin virksomhed kan foretage behandling af de i stk. 1 nævnte oplysninger om organisationens medlemmer eller personer, der på grund af organisationens formål er i regelmæssig kontakt med denne. Videregivelse af sådanne oplysninger kan dog kun finde sted, hvis den registrerede har meddelt sit udtrykkelige samtykke hertil, eller behandlingen er omfattet af stk. 2, nr. 2-4, eller stk. 3.

[240] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 215-238.
[241] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[242] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.

Persondatalovens § 7, stk. 4, er baseret på databeskyttelsesdirektivets artikel 8, stk. 2, litra d, hvoraf det følger, at forbuddet i stk. 1 ikke gælder, hvis behandlingen foretages af en stiftelse, en forening eller et andet almennyttigt organ, hvis sigte er af politisk, filosofisk, religiøs eller faglig art, som led i organets legitime aktiviteter og med de fornødne garantier, på betingelse af, at behandlingen alene vedrører organets medlemmer eller personer, der på grund af organets formål er i regelmæssig kontrakt hermed, og at oplysningerne ikke videregives til tredjemand uden den registreredes samtykke.

Det fremgår af præambelbetragtning nr. 33 til databeskyttelsesdirektivet, at oplysninger, som ifølge deres art kan krænke de grundlæggende frihedsrettigheder eller privatlivets fred, ikke må gøres til genstand for behandling uden den registreredes udtrykkelige samtykke; der skal dog udtrykkeligt gives mulighed for undtagelser fra dette forbud for at imødekomme visse behov, bl.a. navnlig i forbindelse med visse foreningers eller stiftelsers legitime aktiviteter, hvis formål er at sikre udøvelsen af grundlæggende frihedsrettigheder.

Det fremgår af bemærkningerne til persondataloven, at organisationens sigte skal forstås bredt. Omfattet af bestemmelsen vil således være ikke-kommercielle organisationer, som må anses for at have en samfundsmæssig betydning. Dette vil bl.a. kunne være tilfældet for så vidt angår sammenslutninger af personer med samme seksuelle baggrund eller sygdom eller sammenslutninger, der beskæftiger sig med f.eks. indvandrer- eller flygtningespørgsmål.[243]

En fagforening vil også være omfattet af bestemmelsen i persondatalovens § 7, stk. 4, se hertil bl.a. en sag fra Datatilsynet vedrørende spørgsmål om videregivelse af medlemsoplysninger, hvor tilsynet udtalte, at ifølge § 7, stk. 4, kan en fagforening inden for rammerne af sin virksomhed behandle oplysninger om bl.a. medlemmernes fagforeningsmæssige tilhørsforhold.[244]

Det fremgår endvidere af bemærkningerne, at den behandling, som finder sted i organisationer, der falder ind under bestemmelsen, kun må foretages, hvis den vedrører organisationens medlemmer eller personer, der på grund af organisationens formål er i regelmæssig kontakt med denne. Hvorvidt en person er at anse for medlem af en organisation, skal afgøres efter en konkret vurdering, hvori bl.a. vil kunne indgå organisationens vedtægter,

[243] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[244] Sag vedrørende spørgsmål om videregivelse af medlemsoplysninger, Datatilsynets j.nr. 2004-216-0203.

almindelige foreningsretlige regler mv. Hvis den registrerede har meldt sig ud af foreningen, må behandling naturligvis ikke finde sted.[245]

Endelig fremgår det af bemærkningerne til persondataloven, at i kravet om, at behandlingen af oplysninger skal ligge inden for rammerne af organisationens virksomhed, ligger, at der skal være tale om behandling af oplysninger, som ikke står i modstrid med organisationens formål, således som dette måtte fremgå af bl.a. organisationens vedtægter.[246]

Fra Datatilsynets praksis kan nævnes en sag vedrørende Socialdemokraternes anvendelse af medlemsoplysninger, hvori Socialdemokraterne anmodede Datatilsynet om at tage stilling til, hvorvidt organisationen ville kunne udsende markedsføringsmateriale på vegne af virksomheder og organisationer uden samtykke fra det enkelte medlem. Datatilsynet udtalte, at Socialdemokraternes behandling af medlemsoplysninger til udsendelse af markedsføringsmateriale på vegne af virksomheder og organisationer kunne ske efter persondatalovens § 7, stk. 4, 1. pkt., og § 5, stk. 2, hvis denne behandling vurderedes at ligge inden for rammerne af organisationens formål. Om der i en given situation kunne behandles medlemsoplysninger til udsendelse af markedsføringsmateriale, måtte således efter Datatilsynets opfattelse bero på en konkret vurdering af det pågældende markedsføringsmateriale sammenholdt med organisationens virksomhed og formål, herunder organisationens vedtægter.

3.8.2.5. Persondatalovens § 7, stk. 2, nr. 3 (der svarer til databeskyttelsesforordningens artikel 9, stk. 2, litra e)

Det følger af persondatalovens § 7, stk. 2, nr. 3, at behandling af følsomme oplysninger må finde sted, hvis behandlingen vedrører oplysninger, som er blevet offentliggjort af den registrerede.

Bestemmelsen svarer stort set til artikel 8, stk. 2, litra e, 1. led, i databeskyttelsesdirektivet, hvoraf det fremgår, at behandling af følsomme oplysninger må finde sted, hvis behandlingen vedrører oplysninger, som klart offentliggøres af den registrerede.

Det fremgår af bemærkningerne til persondataloven, at bestemmelsens tidsmæssige udstrækning er begrænset til det tidspunkt, hvor den oplysning, der ønskes behandlet, er of-

[245] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[246] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.

fentliggjort af den registrerede. Det er dermed ikke tilstrækkeligt, at den dataansvarlige er bekendt med, at visse personoplysninger er bestemt til offentliggørelse.[247]

Det fremgår endvidere af bemærkningerne, at offentliggørelse i bestemmelsens forstand foreligger, hvis oplysningerne er bragt til kundskab hos en bredere kreds af personer. Dette vil eksempelvis være tilfældet, hvis oplysningerne viderebringes gennem tv, aviser og lignende landsdækkende medier. Også andre former for videregivelse af oplysninger vil kunne anses for offentliggørelse i bestemmelsens forstand.[248]

Derudover vil der også være tale om en offentliggørelse, såfremt dette sker via internettet, på eksempelvis Facebook, Twitter og You Tube. Såfremt den kreds, som får kendskab til oplysningerne, er lukket, er oplysningerne ikke offentliggjort. Eksempelvis vil oplysninger på Facebook, som gives til en reel vennekreds, hvor enhver ikke kan få adgang, ikke anses som værende offentliggjort, hvorimod oplysninger på Facebook, hvor enhver der måtte ønske det kan få adgang, vil meget tale for at anse oplysningerne for offentliggjort.[249]

Fra praksis kan nævnes en sag fra Folketingets Ombudsmand, hvor SKAT brugte en medarbejders private Facebook-profil til at indsamle oplysninger om en kvinde fra hendes Facebook-profil. Kvinden havde en åben profil, hvilket indebar, at alle brugere af Facebook kunne se de oplysninger, der lå om hende på Facebook. Kvinden følte sit privatliv krænket og klagede til Datatilsynet, som sendte klagen videre til Folketingets Ombudsmand. Ombudsmanden udtalte bl.a., at hvis en person har en så åben profil på Facebook, at alle brugere af Facebook kan se de oplysninger, der ligger om personen, er der i realiteten tale om, at oplysningerne er offentligt tilgængelige. Det samme kan efter omstændighederne være tilfældet, hvis en person, som i øvrigt har begrænset tilgængelighed til sin Facebook, har et meget stort antal "venner" på Facebook. Også i dette tilfælde kan oplysningerne om personen blive offentligt tilgængelige. Personoplysninger, som er blevet offentliggjort af den registrerede, kan som udgangspunkt frit behandles af myndighederne, jf. persondatalovens § 7, stk. 2, nr. 3.[250]

[247] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[248] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[249] Persondataloven med kommentarer (2015), s. 290.
[250] Sag vedrørende, at myndigheder må bruge oplysninger fra åbne Facebook-profiler, Folketingets Ombudsmands j.nr. 2011 15-1.

Det er endelig en betingelse, at oplysningerne er offentliggjort på den registreredes foranledning. Oplysninger, som andre, eksempelvis pressen, af egen drift har offentliggjort, er således ikke omfattet.[251]

Fra Datatilsynets praksis om persondatalovens § 7, stk. 2, nr. 3, kan nævnes en klagesag om offentliggørelse på Redox' hjemmeside, hvor Datatilsynet ikke fandt, at der var grundlag for at konkludere, at behandlingen af oplysninger om den registrerede på www.redox.dk havde været i strid med persondatalovens § 7, stk. 2, nr. 3. Datatilsynet lagde navnlig vægt på, at den registrerede selv forudgående, bl.a. i medier, havde offentliggjort oplysninger om sine politiske anskuelser og vurdering af foreningsmæssige forhold i forbindelse hermed, og at den registrerede herunder direkte omtalte forskellige grupperinger og personer i den forening eller det netværk, som den registrerede ifølge det oplyste selv havde været aktiv i.[252]

3.8.2.6. Persondatalovens § 7, stk. 2, nr. 4 (der svarer til databeskyttelsesforordningens artikel 9, stk. 2, litra f)

Det følger af persondatalovens § 7, stk. 2, nr. 4, at behandling af følsomme oplysninger må finde sted, hvis behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

Bestemmelsen svarer til artikel 8, stk. 2, litra e, 2. led, i databeskyttelsesdirektivet.

Det fremgår af bemærkningerne til persondataloven, at bestemmelsen omhandler såvel behandling, der sker i den dataansvarliges interesse, som behandling, der sker i den registreredes interesse. Også behandling af oplysninger, der er nødvendig for, at en tredjemands retskrav kan fastlægges mv., vil kunne ske i henhold til bestemmelsen.[253]

Det fremgår som anført af bemærkningerne, at bl.a. den situation, at behandling af oplysninger om den registrerede er nødvendig for, at den dataansvarlige kan afgøre, om den registrerede har et retskrav, er omfattet af bestemmelsen. Dette vil bl.a. være tilfældet med hensyn til offentlige myndigheders behandling af oplysninger som led i myndighedsudøvelse. Det gælder f.eks. i den situation, hvor de sociale myndigheder har mistanke om incest eller andre seksuelle overgreb mod børn og i den forbindelse ønsker at kontakte andre myndigheder, såsom sygehuse, politi mv., for at beskytte børnene. Nævnes kan endvidere arbejdsgiveres behandling af helbredsoplysninger med henblik på at afgøre, om den

[251] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[252] Afgørelse i klagesag om offentliggørelse på Redox' hjemmeside, Datatilsynets j.nr. 2007-229-0002.
[253] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.

registrerede har krav på erstatning. Dette vil ligeledes gælde for eksempelvis forsikringsselskabers behandling af helbredsoplysninger med henblik på at vurdere, om den registrerede har krav på erstatning. Det fremgår endvidere af bemærkningerne til persondataloven, at det gælder den behandling af oplysning om bl.a. folketingskandidaters politiske overbevisning, som sker i "det fælleskommunale valgopgørelsessystem", og som har til formål at lette administrationen i bl.a. kommunerne i forbindelse med opgørelse af resultatet af kommunale valg og folketingsvalg.[254]

Det fremgår endvidere uddybende af bemærkningerne, at den situation, at behandling af oplysninger om den registrerede er nødvendig for, at det kan afgøres, hvorvidt den dataansvarlige kan gøre et krav gældende over for den registrerede, er omfattet af bestemmelsen. Som eksempel herpå kan nævnes skattemyndighedernes behandling af oplysninger om medlemsskab af folkekirken, der registreres i CPR med henblik på opkrævning af kirkeskatter.[255]

Endelig fremgår det af bemærkningerne til persondataloven, at den situation, at behandlingen er nødvendig for, at en tredjemands retskrav kan fastlægges, gøres gældende eller forsvares, som nævnt også er omfattet. En betingelse herfor er dog yderligere, at kravet om saglighed, jf. § 5, stk. 2, er opfyldt. Dette vil bl.a. være tilfældet i forbindelse med en dataansvarlig domstols behandling af oplysninger om andre personer end parterne, der er nødvendig for afgørelsen af en retssag.[256]

I sag U.2017.1294H, udtalte Højesteret sig bl.a. om, hvorvidt en videregivelse af en persons helbredsoplysninger til dennes arbejdsgiver var berettiget efter persondataloven. Vallensbæk Kommune ønskede at vurdere, hvorvidt refusion af sygedagpenge for den pågældende person skulle standses. Kommunen videregav i den forbindelse en statusattest om vedkommendes sygdomsforløb til vedkommendes arbejdsgiver. Højesteret fandt, at videregivelsen af oplysninger om vedkommendes helbredsforhold havde været nødvendig for at fastslå, om arbejdsgiveren havde krav på dagpengerefusion under personens fortsatte sygdom, og videregivelsen havde derfor været berettiget efter persondatalovens § 7, stk. 2, nr. 4.

Højesteret lagde særligt vægt på, at beskrivelsen af personens helbredstilstand antoges at svare til, hvad der er forholdsvis almindeligt for en person, der er sygemeldt som følge af

[254] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[255] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[256] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.

en krisetilstand efter en uansøgt afskedigelse. Højesteret lagde endvidere vægt på, at den påtænkte afgørelse om bortfald af dagpengerefusion var bebyrdende for arbejdsgiveren, at arbejdsgiverens ledelse, der modtog oplysningerne, havde tavshedspligt, og at oplysningerne i statusattesten havde væsentlig betydning for arbejdsgiverens mulighed for at vurdere og – eventuelt efter drøftelse med personen – kommentere, om kommunen havde tilstrækkeligt grundlag for at træffe afgørelse om bortfald af personens sygedagpenge.

Ved skrivelse af 11. februar 2000 rettede Kommunernes Landsforening henvendelse til Justitsministeriet vedrørende kommuners og private virksomheders adgang til i forbindelse med udlicitering af sociale opgaver at behandle og herunder videregive følsomme oplysninger efter bl.a. persondatalovens § 7. Baggrunden for spørgsmålene var bl.a., at der i forbindelse med kommunernes udlicitering af sociale opgaver til private virksomheder var behov for et smidigt samarbejde, og at det erfaringsmæssigt ikke altid var muligt at indhente et samtykke fra klienten vedrørende den skitserede dataudveksling mellem kommunen og den private virksomhed. I den forbindelse udtalte Registertilsynet, at vurderingen af, hvorvidt behandling vil kunne finde sted, beror på en konkret vurdering. Registertilsynet udtalte, at behandling af følsomme oplysninger, omfattet af lovforslagets § 7, stk. 1, hvilket i denne sammenhæng først og fremmest var oplysninger om helbredsforhold, efter tilsynets opfattelse kunne ske med hjemmel i lovforslagets § 7, stk. 2, nr. 4. Tilsynet forudsatte, at der var tale om ydelser, som de personer, om hvem der behandledes oplysninger, havde retskrav på at modtage.[257]

Fra praksis kan endvidere nævnes en sag vedrørende behandling af oplysninger hos Projekt Janus, som drejede sig om et socialt projekt med behandling af unge, som havde været seksuelt krænkende over for børn. I den forbindelse skulle der behandles oplysninger om ofrene, herunder om deres alder, køn, relation til krænkeren samt oplysninger om seksuelle forhold på baggrund af krænkerens oplysninger. I den forbindelse udtalte Projekt Janus, at de anså det for nødvendigt at inddrage oplysninger om ofret i behandlingen, idet det ikke kunne udelukkes, at sådanne oplysninger spillede en afgørende rolle for at kunne udlede baggrunden for den pågældende krænkelse og dermed for behandlingen af krænkeren, således at gentagelsessituationer blev undgået. Datatilsynet udtalte i den forbindelse, at oplysninger om ofret med hjemmel i persondatalovens § 7, stk. 2, nr. 4, kunne behandles uden samtykke, hvis det ud fra en konkret vurdering viste sig nødvendigt for at kunne give krænkeren den bedst mulige behandling. I den forbindelse lagde Datatilsynet vægt på reglerne i lov om social service om støtteforanstaltninger til børn og unge.[258]

[257] Refereret i forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, bilag 52 fra Retsudvalget.
[258] Sag vedrørende behandling af oplysninger hos Projekt Janus, Datatilsynets j.nr. 2004-54-1508.

Endvidere udtalte Datatilsynet i en sag vedrørende behandling af personoplysninger i et konkursbo, at det efter tilsynets opfattelse næppe kunne afvises generelt, at reglen i persondatalovens § 7, stk. 2, nr. 4, i visse tilfælde kunne give grundlag for kurators behandling af følsomme oplysninger. Efter persondatalovens § 7, stk. 2, nr. 4, kunne behandling af personoplysninger foretages, såfremt behandlingen var nødvendig for, at et retskrav kunne fastlægges, gøres gældende eller forsvares.[259]

3.8.2.7. Databeskyttelsesdirektivets artikel 8, stk. 4 (der svarer til databeskyttelsesforordningens artikel 9, stk. 2, litra g, i og j)
Det fremgår af databeskyttelsesdirektivets artikel 8, stk. 4, at med forbehold af, at der gives tilstrækkelige garantier, kan medlemsstaterne af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, fastsætte andre undtagelser end dem, der er nævnt i stk. 2, enten ved national lovgivning eller ved en afgørelse truffet af tilsynsmyndigheden.

Det fremgår endvidere af databeskyttelsesdirektivets artikel 8, stk. 6, at undtagelser fra stk. 1, som omhandlet i stk. 4 og 5, meddeles til Kommissionen.

Det fremgår af præambelbetragtning nr. 34 til databeskyttelsesdirektivet, at når hensynet til vigtige samfundsmæssige interesser berettiger det, skal medlemsstaterne ligeledes kunne fravige forbuddet mod at behandle følsomme kategorier af data på områder som f.eks. folkesundhed og social sikring – navnlig for at sikre kvaliteten og rentabiliteten af de procedurer, der anvendes i forbindelse med ansøgninger om ydelser og tjenester inden for en sygesikringsordning – videnskabelig forskning og offentlig statistik; det påhviler imidlertid medlemsstaterne at sørge for de fornødne specifikke garantier for beskyttelsen af det enkelte menneskes grundlæggende rettigheder og privatliv.

Det fremgår desuden af præambelbetragtning nr. 35 til databeskyttelsesdirektivet, at offentlige myndigheders behandling af personoplysninger for officielt anerkendte religiøse sammenslutninger for at opfylde mål, der er fastsat i forfatningsretten eller i folkeretten, udføres af hensyn til vigtige samfundsmæssige interesser.

Det fremgår endvidere af præambelbetragtning nr. 36 til databeskyttelsesdirektivet, at hvis det i forbindelse med afholdelse af valg i visse medlemsstater er nødvendigt for at det demokratiske system kan fungere, at politiske partier indsamler oplysninger om enkeltpersoners politiske holdning, kan behandling af sådanne oplysninger tillades af hensyn til varetagelsen af vigtige samfundsmæssige interesser, forudsat, at der fastsættes bestemmelser om de fornødne garantier.

[259] Sag vedrørende behandling af personoplysninger i konkursbo, Datatilsynets j.nr. 2003-215-0131.

I Danmark ses der i særlovgivning kun i begrænset omfang vedtaget undtagelser til databeskyttelsesdirektivets artikel 8, stk. 1, inden for det råderum som direktivets artikel 8, stk. 4, overlader medlemsstaterne. Et eksempel herpå er bl.a. reglerne i persondatalovens §§ 9 og 10, som omhandler henholdsvis behandling af oplysninger i retsinformationssystemer og behandling af oplysninger med henblik på udførelse af statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning.

Derudover skal persondatalovens § 7, stk. 7, ses i lyset af direktivets artikel 8, stk. 4.

Det fremgår af persondatalovens § 7, stk. 7, at undtagelse fra bestemmelsen i stk. 1 endvidere kan gøres, hvis behandlingen af oplysninger sker af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser. Tilsynsmyndigheden giver tilladelse hertil. Der kan fastsættes nærmere vilkår for behandlingen. Hvor tilladelse meddeles, giver tilsynsmyndigheden underretning herom til Kommissionen.

Persondatalovens § 7, stk. 7, er delvist baseret på databeskyttelsesdirektivets artikel 8, stk. 4, hvorefter medlemsstaterne med forbehold af, at der gives tilstrækkelige garantier, af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, kan fastsætte andre undtagelser end dem, der er nævnt i artikel 8, stk. 2, ved afgørelse truffet af tilsynsmyndigheden.

Det fremgår af bemærkningerne til persondataloven, at § 7, stk. 7, der skal ses i lyset af direktivets artikel 8, stk. 4, tager sigte på behandling af oplysninger, som ikke er hjemlet i bestemmelserne i stk. 2-6. I givet fald kan behandling kun ske efter indhentet tilladelse fra vedkommende tilsynsmyndighed. I de tilfælde, hvor tilladelse meddeles, kan tilsynsmyndigheden fastsætte, under hvilke nærmere betingelser behandlingen må finde sted. Det påhviler tilsynsmyndigheden at foretage den fornødne underretning af Kommissionen med hensyn til de tilladelser, som meddeles i henhold til bestemmelsen. Herved sikres, at bestemmelsen i direktivets artikel 8, stk. 6, bliver overholdt.[260]

Det fremgår endvidere af bemærkningerne, at bestemmelsen, der har karakter af en opsamlingsbestemmelse, forudsættes at have et snævert anvendelsesområde. Det anføres desuden, at det er vanskeligt – på forhånd – at angive eksempler på eventuelle undtagelsestilfælde, der vil være omfattet af bestemmelsen i lovforslagets § 7, stk. 7, hvorfor det således må overlades til tilsynsmyndigheden (Datatilsynet) i det konkrete tilfælde at foretage en

[260] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.

vurdering af, om behandling af oplysninger kan tillades af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, og om der bør fastsættes vilkår for behandlingen.[261]

Det fremgår endelig af bemærkningerne til persondataloven, at i det omfang, der i lovgivningen er fastsat særlige regler, hvorefter behandling af oplysninger kan ske af hensyn til nærmere angivne vigtige samfundsmæssige interesser, vil vedkommende tilsynsmyndigheds tilladelse til behandlingen ikke skulle indhentes. Derimod vil Kommissionen skulle underrettes om eksistensen af sådanne lovregler, jf. artikel 8, stk. 6.[262]

Bestemmelsen blev første gang anvendt af Datatilsynet i 2011 i en sag vedrørende et rådgivningscenters behandling af følsomme oplysninger om pårørende.[263]

3.8.2.8. Persondatalovens § 7, stk. 5 (der svarer til databeskyttelsesforordningens artikel 9, stk. 2, litra h)

Det fremgår som nævnt af persondatalovens § 7, stk. 1, at der ikke må behandles oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

Det følger imidlertid af persondatalovens § 7, stk. 5, at bestemmelsen i stk. 1, ikke finder anvendelse - det vil sige, at behandling af oplysninger nævnt stk. 1 alligevel må ske - hvis behandlingen af oplysningerne er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

Persondatalovens § 7, stk. 5, oplister således en række (fakultative) formål, hvortil behandling af følsomme personoplysninger kan ske, når det er nødvendigt for at opfylde et eller flere af de pågældende formål. Fælles for de oplistede formål er, at de omhandler behandling af oplysninger på sundhedsområdet. Kravet om nødvendighed forudsætter en konkret vurdering, som er baseret på et vist skøn.

Endvidere er det ifølge bestemmelsen en betingelse, at de personer, der behandler oplysninger, udfører aktiviteter inden for sundhedssektoren og er undergivet tavshedspligt i henhold til lovgivningen.

[261] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[262] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7.
[263] Omtalt i Datatilsynets årsberetning 2011, s. 25.

Bestemmelsen i persondatalovens § 7, stk. 5, gennemfører artikel 8, stk. 3, i databeskyttelsesdirektivet, og ordlyden af persondatalovens § 7, stk. 5, svarer til ordlyden af direktivet.

Det fremgår af databeskyttelsesdirektivets præambelbetragtning nr. 33, at oplysninger, som ifølge deres art kan krænke de grundlæggende frihedsrettigheder eller privatlivets fred, ikke må gøres til genstand for behandling uden den registreredes udtrykkelige samtykke, men at der dog udtrykkeligt skal gives mulighed for undtagelser fra dette forbud for at imødekomme visse behov, navnlig i sådanne tilfælde, hvor databehandlingen udføres med bestemte sundhedsmæssige formål og af personer, der er underkastet tavshedspligt.

Endvidere fremgår det af præambelbetragtning nr. 34, at medlemsstaterne skal kunne fravige forbuddet mod at behandle følsomme kategorier af data på områder som f.eks. folkesundhed og social sikring, navnlig for at sikre kvaliteten og rentabiliteten af de procedurer, der anvendes i forbindelse med ansøgninger om ydelser og tjenester inden for en sygesikringsordning.

Det fremgår af bemærkningerne til persondatalovens § 7, stk. 5, og registerudvalgets betænkning nr. 1345, at der i databeskyttelsesdirektivets artikel 8, stk. 3, er fastsat særlige regler for, i hvilket omfang behandling af de i artiklens stk. 1 nævnte typer af følsomme personoplysninger kan finde sted inden for sundhedssektoren, og at det må antages, at direktivets artikel 8, stk. 3, omfatter behandling af oplysninger, som er nødvendige af hensyn til varetagelsen af aktiviteter inden for sundhedssektoren. Der er navnlig tale om aktiviteter, som foretages på sygehuse, klinikker og hos læger, men bestemmelsen omfatter også særlige institutioner i privat eller offentlig regi, hjemmesygepleje samt tildeling af hjælpemidler og lignende tiltag, som udgør en opfølgning på en behandling. Herudover omfattes behandling af oplysninger med henblik på varetagelsen af de administrative opgaver, som er nødvendige i forbindelse med forvaltningen af sådanne institutioner.[264]

Endvidere fremgår det, at persondatalovens § 7, stk. 5 – der som nævnt gennemfører databeskyttelsesdirektivets artikel 8, stk. 3 – indebærer, at den dataansvarlige vil kunne behandle de i persondatalovens § 7, stk. 1, nævnte oplysninger i forbindelse med varetagelsen af sine opgaver på sundhedsområdet, og at den for patientbehandlingen nødvendige behandling af oplysninger om f.eks. seksuelle forhold eller helbredsforhold, herunder om misbrug af nydelsesmidler, således vil kunne finde sted. Det fremgår tillige, at behandling af personoplysninger, som er nødvendig for at følge op på en egentlig patientbehandling, f.eks. gennem offentlig støtte i form af hjælpemidler mv., er omfattet af bestemmelsen,

[264] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7 og Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 246 ff.

ligesom bestemmelsen omfatter dataansvarliges løsning af deres administrative opgaver på det sundhedsmæssige område.[265]

Endelig fremgår det af bemærkningerne til persondataloven og Registerudvalgets betænkning nr. 1345, at betingelsen om tavshedspligt i almindelighed vil være opfyldt i relation til de personer, som normalt behandler følsomme personoplysninger inden for sundhedssektoren. Dette baseres ifølge bemærkningerne og betænkningen bl.a. på dansk rets almindelige regler om tavshedspligt, jf. straffelovens § 152 og §§ 152 a-152 f, hvorefter bl.a. personale hos offentlige myndigheder, herunder offentlige sygehuse, er undergivet tavshedspligt, ligesom den som i øvrigt er eller har været beskæftiget med opgaver, der udføres efter aftale med en offentlig myndighed, eller personer, som udøver deres virksomhed efter autorisation fra det offentlige, f.eks. læger, vil være undergivet tavshedspligt efter reglerne. Endvidere baseres det på tavshedspligtsregler, der særligt retter sig mod personer inden for sundhedsområdet.[266]

3.8.3. Databeskyttelsesforordningen

Det fremgår af Kommissionens oprindelige forslag til databeskyttelsesforordningen, at der i artikel 9 fastsættes det generelle forbud mod behandling af særlige kategorier af personoplysninger og undtagelserne fra denne generelle regel baseret på artikel 8 i databeskyttelsesdirektivet.[267]

I databeskyttelsesforordningens artikel 9, stk. 1, oplistes, hvilke personoplysninger, som er særlige, og derfor som udgangspunkt ikke må behandles, mens artikel 9, stk. 2, anfører, hvornår der alligevel er hjemmel til behandling af sådanne særlige kategorier af oplysninger. Efter bestemmelsen er det som behandlingshjemmel kun nødvendigt, at ét af forholdene i stk. 2, gør sig gældende, for at behandling af oplysninger omfattet af forordningens artikel 9, stk. 1, kan behandles.

Databeskyttelsesforordningens artikel 9, stk. 1, indeholder således udgangspunktet om, at behandling af følsomme oplysninger er forbudt, mens artikel 9, stk. 2, indfører en række undtagelser, hvorefter der alligevel vil kunne ske behandling af de følsomme oplysninger.

Databeskyttelsesforordningens artikel 9, stk. 2, litra a, c, d, e og f, kan efter deres ordlyd anvendes som direkte behandlingshjemler, så længe behandlingsbetingelserne i de pågæl-

[265] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7 og Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 246 ff.
[266] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7 og Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 246 ff.
[267] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig).

dende bestemmelser er opfyldt, f.eks. hvis behandlingen sker af hensyn til "den registreredes eller en anden fysisk persons vitale interesser", jf. litra c.

Heroverfor synes artikel 9, stk. 2, litra b, g, h, i og j med henvisninger – dog med forskellig formulering – til EU-retten eller medlemsstaternes nationale ret, at forudsætte, at behandlingen er forankret i f.eks. national ret for, at udgangspunktet i artikel 9, stk. 1, om forbud mod behandling af følsomme oplysninger, kan fraviges. Det fremgår om disse litraer i præambelbetragtning nr. 52, 1. pkt., at "[d]er bør også gives mulighed for at fravige forbuddet mod at behandle særlige kategorier af personoplysninger, når det er fastsat i EU-retten eller medlemsstaternes nationale ret og er omfattet af de fornødne garantier". Se nærmere om denne mulighed for national lovgivning nedenfor.

Som efter persondatalovens § 7 og artikel 8, stk. 2, i databeskyttelsesdirektivet, vil det for de bestemmelser i databeskyttelsesforordningens artikel 9, stk. 2, som har et krav om nødvendighed, bero på den konkrete situation, hvorvidt en given behandling af oplysninger må antages at være nødvendig i bestemmelsens forstand. Med kravet om, at behandlingen skal være nødvendig, er der således overladt et vist skøn til den dataansvarlige.

Det fremgår af præambelbetragtning nr. 51, at følsomme personoplysninger ikke bør behandles, medmindre behandling er tilladt i specifikke tilfælde, der er fastsat i denne forordning, under hensyntagen til at medlemsstaternes nationale ret kan fastsætte specifikke bestemmelser om databeskyttelse for at tilpasse anvendelsen af reglerne i denne forordning med henblik på overholdelse af en retlig forpligtelse eller udførelse af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Foruden de specifikke krav til sådan behandling bør de generelle principper og andre regler i denne forordning finde anvendelse, navnlig for så vidt angår betingelserne for lovlig behandling. Der bør udtrykkelig gives mulighed for undtagelser fra det generelle forbud mod behandling af sådanne særlige kategorier af personoplysninger, bl.a. hvis den registrerede giver sit udtrykkelige samtykke eller for så vidt angår specifikke behov, navnlig hvis behandling foretages i forbindelse med visse sammenslutningers eller stiftelsers legitime aktiviteter, hvis formål er at muliggøre udøvelse af grundlæggende frihedsrettigheder.

3.8.3.1. Databeskyttelsesforordningens artikel 9, stk. 2, litra a

Det fremgår af forordningens artikel 9, stk. 2, litra a, at behandling af følsomme oplysninger er lovlig, hvis den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål, medmindre det i EU-retten eller medlemsstaternes nationale ret er fastsat, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke.

Bestemmelsen i forordningens artikel 9, stk. 2, litra a, svarer efter ordlyden til bestemmelsen i databeskyttelsesdirektivets artikel 8, stk. 2, litra a, som persondatalovens § 7, stk. 2, nr. 1, er baseret på.

Både i databeskyttelsesforordningens artikel 9, stk. 2, litra a, i databeskyttelsesdirektivets artikel 8, stk. 2, litra a, og i persondatalovens § 7, stk. 1, nr. 1, fremgår det, at samtykket skal være *udtrykkeligt*.

Registerudvalget anførte i betænkning nr. 1345, at der med udtrykket "udtrykkeligt" i databeskyttelsesdirektivets artikel 8, stk. 2, litra a, efter udvalgets opfattelse, antages at ligge et krav om, at et samtykke skal være *klart og utvetydigt*. Efter udvalgets opfattelse må kravet om udtrykkelighed antages at føre til, at der ikke er mulighed for, at den dataansvarlige opnår stiltiende eller indirekte tilslutning fra den registrerede.[268]

Efter databeskyttelsesforordningen antages det fortsat ikke, at der er noget skærpet krav til et gyldigt samtykke efter forordningens artikel 9, stk. 2, litra a, i forhold til samtykke efter forordningens artikel 6, stk. 1, litra a, hvilket også skal ses i sammenhæng med, at der er adskillige krav til et samtykkes gyldighed i forordningen, se herfor afsnit 2.3. om definitioner samt afsnit 3.5. om betingelser for samtykke, artikel 7. Ordet "udtrykkeligt" i forordningens artikel 9, stk. 2, litra a, understreger dog vigtigheden af, at der ikke må være tvivl om, at der er givet samtykke.

I forordningens artikel 9, stk. 2, litra a, er der en tilføjelse i forhold til gældende ret, idet der er indsat et krav om, at samtykket skal være til et eller flere specifikke formål. At dette nu er indsat i artikel 9, stk. 2, litra a, vil kun være en præcisering af, hvad der er gældende ret, idet dette specifikationskrav til et samtykke allerede følger af kravene til et gyldigt samtykke i persondatalovens § 3, nr. 8.

At der er indsat en eksplicit henvisning til, at formålet skal specificeres, stemmer overens med, at samtykkets omfang fortsat må skulle fortolkes ligesom efter gældende ret, hvor det netop i forbindelse med vurderingen af samtykkets gyldighed skal tillægges betydning, hvilken form for personoplysninger, der behandles. Det præciseres således, at det er endnu vigtigere at iagttage hensynet til, at et samtykke skal være specifikt, når der behandles følsomme oplysninger.

Det kan herefter konkluderes, at forordningens artikel 9, stk. 2, litra a, er en videreførelse af gældende ret.

[268] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 215-216.

I databeskyttelsesforordningens artikel 9, stk. 2, litra a, er der mulighed for, at det i EU-retten og medlemsstaterne nationale ret kan fastsættes, at forbuddet mod behandling af følsomme oplysninger ikke kan hæves ved den registreredes samtykke. Databeskyttelsesdirektivet indeholder en tilsvarende mulighed.

Databeskyttelsesforordningens artikel 9, stk. 2, litra a, fastslår således, at der fortsat er denne mulighed for at udelukke, at samtykke kan anvendes som behandlingshjemmel i forbindelse med behandling af følsomme oplysninger.

3.8.3.2. Databeskyttelsesforordningens artikel 9, stk. 2, litra b

Det fremgår af databeskyttelsesforordningens artikel 9, stk. 2, litra b, at behandling af følsomme oplysninger er lovlig, hvis behandling er nødvendig for at overholde den dataansvarliges eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder, for så vidt den har hjemmel i EU-retten eller medlemsstaternes nationale ret eller en kollektiv overenskomst i medfør af medlemsstaternes nationale ret, som giver fornødne garantier for den registreredes grundlæggende rettigheder og interesser.

Den del af databeskyttelsesforordningens artikel 9, stk. 2, litra b, som vedrører arbejdsretlige forpligtelser og specifikke rettigheder, svarer efter ordlyden i vidt omfang til databeskyttelsesdirektivets artikel 8, stk. 2, litra b, og persondatalovens § 7, stk. 3.

Dog fremgår det yderligere, at der i databeskyttelsesforordningens artikel 9, stk. 2, litra b, er mulighed for at tillægge den *registreredes* forpligtelser og specifikke rettigheder betydning – modsat kun den *dataansvarliges* forpligtelser og specifikke rettigheder efter databeskyttelsesdirektivet.

Vedrørende det sundheds- og socialretlige område, er der tale om en præcisering i forhold til gældende ret, idet der nu direkte i bestemmelsen vedrørende følsomme oplysninger er hjemmel til at fastsætte EU-regler eller nationale regler for behandlingen.

Efter databeskyttelsesforordningens artikel 9, stk. 2, litra b, er det kun muligt at fastsætte regler om lovlig behandling af følsomme oplysninger på det arbejds-, sundheds- og socialretlige område. Dette stemmer godt overens med, at det typisk netop er inden for disse områder, at oplysninger er særligt beskyttede som følsomme efter forordningens artikel 9, stk. 1, ligesom det også stemmer godt overens med, at der er en videre beskyttelse ved behandling af følsomme oplysninger i forhold til almindelige personoplysninger. Behandling inden for andre områder end det arbejds-, sundheds- og socialretlige område vil dog kunne ske efter bestemmelserne i databeskyttelsesforordningens artikel 9, stk. 2, litra g eller j.

Det fremgår som fortolkningsbidrag til artikel 9, stk. 2, litra b, af præambelbetragtning nr. 52, at der også bør gives mulighed for at fravige forbuddet mod at behandle særlige kategorier af personoplysninger, når det er fastsat i EU-retten eller medlemsstaternes nationale ret og er omfattet af de fornødne garantier, således at personoplysninger og andre grundlæggende rettigheder beskyttes, hvis dette er i samfundets interesse, navnlig behandling af personoplysninger inden for ansættelsesret, socialret, herunder pensioner og med henblik på sundhedssikkerhed, overvågning og varsling, forebyggelse eller kontrol af overførbare sygdomme og andre alvorlige trusler mod sundheden.

Det fremgår endvidere af præambelbetragtning nr. 52, at en sådan fravigelse kan ske til sundhedsformål, herunder folkesundhed og forvaltning af sundhedsydelser, især for at sikre kvaliteten og omkostningseffektiviteten af de procedurer, der anvendes til afregning i forbindelse med ydelser og tjenester inden for sygesikringsordninger, eller til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål.

Forordningens artikel 9, stk. 2, litra b, indeholder det yderligere krav, at lovgivningen eller overenskomsterne skal give de fornødne garantier for den registreredes grundlæggende rettigheder og interesser. Efter databeskyttelsesdirektivets artikel 8, stk. 1, litra b, skulle der også fastsættes "fornødne garantier". Ved fastsættelsen af regler eller overenskomster skal der derfor tages hensyn til den registreredes grundlæggende rettigheder og interesser, for at behandling vil kunne ske med hjemmel i databeskyttelsesforordningens artikel 9, stk. 2, litra b.

Der henvises i øvrigt til afsnit 10.4. om nærmere analyse af rammerne i artikel 88 vedrørende ansættelsesforhold.

3.8.3.3. Databeskyttelsesforordningens artikel 9, stk. 2, litra c

Det fremgår af forordningens artikel 9, stk. 2, litra c, at behandling af følsomme oplysninger er lovlig, hvis behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke.

Bestemmelsen i forordningens artikel 9, stk. 2, litra c, svarer efter ordlyden til bestemmelsen i databeskyttelsesdirektivets artikel 8, stk. 2, litra c, og persondatalovens § 7, stk. 2, nr. 2.

Forordningens artikel 9, stk. 2, litra c, ses at være i overensstemmelse med gældende ret.

For yderligere herom henvises der til publikations afsnit 3.3. om lovlig behandling af ikke-følsomme oplysninger, artikel 6, stk. 1.

3.8.3.4. Databeskyttelsesforordningens artikel 9, stk. 2, litra d

Det fremgår af databeskyttelsesforordningens artikel 9, stk. 2, litra d, at behandling af følsomme oplysninger er lovlig, hvis behandling foretages af en stiftelse, en sammenslutning eller et andet organ, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art, som led i organets legitime aktiviteter og med de fornødne garantier, og på betingelse af at behandlingen alene vedrører organets medlemmer, tidligere medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed, og at personoplysningerne ikke videregives uden for organet uden den registreredes samtykke.

Det fremgår af præambelbetragtning nr. 51, at der udtrykkeligt bør gives mulighed for undtagelser fra det generelle forbud mod behandling af sådanne særlige kategorier af personoplysninger bl.a. navnlig, hvis behandling foretages i forbindelse med visse sammenslutningers eller stiftelsers legitime aktiviteter, hvis formål er at muliggøre udøvelse af grundlæggende frihedsrettigheder.

Ordlyden i databeskyttelsesforordningens artikel 9, stk. 2, litra d, ses næsten at være identisk med databeskyttelsesdirektivets artikel 8, stk. 2, litra d, som persondatalovens § 7, stk. 4, er baseret på. Det antages ikke, at den ændrede formulering af persondatalovens § 7, stk. 4, har bevirket, at bestemmelsen har været tiltænkt et andet anvendelsesområde end artikel 8, stk. 2, litra d, i databeskyttelsesdirektivet – og hermed gældende ret. Selvom persondatalovens § 7, stk. 4, ikke eksplicit nævner *som led i organets legitime interesser* og *med de fornødne garantier,* må det lægges til grund, at et sådant krav også vil gælde for behandlingen efter persondatalovens § 7, stk. 4, idet bestemmelsen netop er baseret på databeskyttelsesdirektivets artikel 8, stk. 2, litra d. Som udgangspunkt vil forordningens artikel 9, stk. 2, litra d, derfor have samme anvendelsesområde som gældende ret.

I databeskyttelsesforordningens artikel 9, stk. 2, litra d, er der en tilføjelse i forhold til databeskyttelsesdirektivets artikel 8, stk. 2, litra d, og persondatalovens § 7, stk. 4, idet det af bestemmelsen fremgår, at der skal være tale om en stiftelse, en sammenslutning eller et andet organ, *som ikke arbejder med gevinst for øje*. Som anført ovenfor fremgår det af bemærkningerne til persondatalovens § 7, stk. 4, at omfattet af bestemmelsen vil være ikke-kommercielle organisationer, som må anses for at have en samfundsmæssig betydning. Dette ses at harmonere med, hvad der nu fremgår af databeskyttelsesforordningens artikel 9, stk. 2, litra d, hvorfor præciseringen heri blot ses at være en videreførelse af gældende ret.

Endvidere er der i databeskyttelsesforordningens artikel 9, stk. 2, litra d, en tilføjelse i forhold til databeskyttelsesdirektivets artikel 8, stk. 2, litra d, idet det er tilføjet, at også behandling, som vedrører *tidligere medlemmer*, vil være omfattet af bestemmelsen. Modsat dette fremgår det af bemærkningerne til persondatalovens § 7, stk. 4, at hvis den registrerede har meldt sig ud af foreningen, må behandling naturligvis ikke finde sted. Med tilføjelsen af behandling vedrørende tidligere medlemmer i forordningens artikel 9, stk. 2, litra d, vil der derfor være tale om en ændring i forhold til gældende ret, idet det nu klart fremgår af bestemmelsen, at denne også omfatter tidligere medlemmer.

Overordnet ses forordningens artikel 9, stk. 2, litra d, således at være i overensstemmelse med gældende ret – dog vil bestemmelsen efter forordningens ikrafttrædelse nu også vedrøre tidligere medlemmer. Det bemærkes i den forbindelse, at de grundlæggende principper for behandling af personoplysninger i databeskyttelsesforordningens artikel 5 naturligvis fortsat skal iagttages.

3.8.3.5. Databeskyttelsesforordningens artikel 9, stk. 2, litra e

Det fremgår af forordningens artikel 9, stk. 2, litra e, at behandling af følsomme oplysninger er lovlig, hvis behandling vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede.

Bestemmelsen i forordningens artikel 9, stk. 2, litra e, svarer efter ordlyden til bestemmelsen i databeskyttelsesdirektivets artikel 8, stk. 2, litra e, 1. led – idet der ikke ses at være en forskel på begreberne *tydeligvis* og *klart*. Persondatalovens § 7, stk. 2, nr. 3, er baseret på databeskyttelsesdirektivets artikel 8, stk. 2, litra e, 1. led.

Selvom der i persondatalovens § 7, stk. 2, nr. 3, ikke tales om *tydeligvis*, som det er tilfældet i databeskyttelsesforordningens artikel 9, stk. 2, litra e, kan det ikke antages, at der er forskel på vurderingen herefter. Persondatalovens § 7, stk. 2, nr. 3, er baseret på databeskyttelsesdirektivets artikel 8, stk. 2, litra e, 1. led, hvori der tales om *klart*. Ordet klart ses at have samme indholdsmæssige betydning som ordet tydeligvis, som benyttes i databeskyttelsesforordningen.

Der er derfor ikke grund til at antage, at der skulle være tale om en ændring i forhold til gældende ret.

Forordningens artikel 9, stk. 2, litra e, ses således at være i overensstemmelse med databeskyttelsesdirektivet og en videreførelse af gældende ret.

3.8.3.6. Databeskyttelsesforordningens artikel 9, stk. 2, litra f

Det fremgår af forordningens artikel 9, stk. 2, litra f, at behandling af følsomme oplysninger er lovlig, hvis behandling er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol.

Bestemmelsen i forordningens artikel 9, stk. 2, litra f, svarer efter ordlyden til bestemmelsen i databeskyttelsesdirektivets artikel 8, stk. 2, litra e, 2. led, og persondatalovens § 7, stk. 2, nr. 4.

Det fremgår af præambelbetragtning nr. 52, at en fravigelse desuden bør gøre det muligt at behandle sådanne personoplysninger, hvis det er nødvendigt, for at retskrav kan fastslås, gøres gældende eller forsvares, uanset om det er i forbindelse med en retssag eller en administrativ eller udenretslig procedure.

Som tidligere anført følger det af gældende ret, at den situation, at behandling af oplysninger om den registrerede er nødvendig for, at den dataansvarlige kan afgøre, om den registrerede har et retskrav, er omfattet af bestemmelsen bl.a. vil være tilfældet med hensyn til offentlige myndigheders behandling af oplysninger som led i myndighedsudøvelse.

På baggrund af en ordlydsfortolkning af bestemmelsen ses der ikke at være holdepunkter for, at bestemmelsen ikke længere skulle finde anvendelse i forbindelse med offentlige myndigheders myndighedsudøvelse. Det fremhæves endda i præambelbetragtning nr. 52, at bestemmelsen vil finde anvendelse i disse situationer, idet det fremgår, at bestemmelsen kan anvendes, hvis det er nødvendigt, for at et retskrav kan fastslås i forbindelse med *administrativ procedure.* Bestemmelsens anvendelse i forbindelse med offentlig myndighedsudøvelse ses derfor at være i overensstemmelse med gældende ret. Forordningens artikel 9, stk. 2, litra f, kan således anvendes på offentlig afgørelsesvirksomhed. Det vil endvidere ikke være udelukket, at bestemmelsen kan anvendes inden for faktisk forvaltningsvirksomhed, hvis dette sker for, at et retskrav kan fastlægges, gøres gældende eller forsvares, jf. eksempelvis sagen vedrørende behandling af oplysninger hos Projekt Janus, der er omtalt ovenfor.

I forordningens artikel 9, stk. 2, litra f, er der en tilføjelse i forhold til gældende ret, idet det fremgår, at behandling af følsomme oplysninger også vil være nødvendig*, når domstolene handler i deres egenskab af domstol.*

Vedrørende domstolenes behandling af følsomme oplysninger, fremgår det som ovenfor anført af bemærkningerne til persondataloven, at behandling af oplysninger, der er nødvendig for, at en tredjemands retskrav kan fastlægges mv., bl.a. vil kunne ske i henhold til

persondatalovens § 7, stk. 2, nr. 4, i forbindelse med en dataansvarlig domstols behandling af oplysninger om andre personer end parterne, der er nødvendig for afgørelsen af en retssag.

På denne baggrund ses domstolenes behandling af oplysninger allerede efter gældende ret at være omfattet af bestemmelsen, hvorfor der ikke vil være tale om en ændring af gældende ret med tilføjelsen i databeskyttelsesforordningen.

Forordningens artikel 9, stk. 2, litra f, ses derfor at være i overensstemmelse med gældende ret.

Som anført i afsnit om 3.7. om følsomme oplysninger, artikel 9, stk. 1, bliver biometrisk data med det formål entydigt at identificere en fysisk person – modsat efter gældende ret – når forordningen finder anvendelse fra den 25. maj 2018, omfattet af den særlige kategori af personoplysninger i artikel 9, stk. 1. Eksempelvis vil templates (fingeraftryk eller en matematisk værdi af et fingeraftryk) efter forordningen skulle behandles som følsomme oplysninger, hvorfor sådanne oplysninger ikke længere vil kunne behandles med hjemmel i persondatalovens § 6, stk. 1 – svarende til databeskyttelsesforordningens artikel 6, stk. 1.

Det må antages, at offentlige myndigheder fremadrettet vil kunne anvende fingeraftryk til brug for registrering af borgere med hjemmel i databeskyttelsesforordningens artikel 9, stk. 2, litra f, i det omfang, der skal fastlægges et retskrav, hvis det sker som led i offentlig myndighedsudøvelse. Eksempelvis vil en kommune med hjemmel i artikel 9, stk. 2, litra f, således kunne anvende fingeraftryk ved registrering af aktiverede borgeres fremmøde med det formål at bruge registreringen til udmåling og eventuelt sanktionering af udeblivelser i overensstemmelse med lovgivningen på det sociale område. Det samme vil være tilfældet inden for den private sektor, såfremt der skal fastlægges et retskrav. Det er dog naturligvis en betingelse for behandlingen af biometriske oplysninger, at behandlingen er "nødvendig", jf. kravet herom i forordningens artikel 9, stk. 2, litra f, og myndigheden eller den private virksomhed skal være i stand til kunne påvise nødvendigheden af behandlingen.

3.8.3.7. Databeskyttelsesforordningens artikel 9, stk. 2, litra g

Det fremgår af databeskyttelsesforordningens artikel 9, stk. 2, litra g, at behandling af følsomme oplysninger er lovlig, hvis behandling er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Databeskyttelsesforordningens artikel 9, stk. 2, litra g, svarer efter ordlyden delvist til databeskyttelsesdirektivets artikel 8, stk. 4. Dog gælder der ikke efter forordningens artikel 9, stk. 2, litra g, som ved databeskyttelsesdirektivets artikel 8, stk. 4, i medfør af direktivets artikel 8, stk. 6, et krav om, at undtagelser efter bestemmelsen skal meddeles til Kommissionen, ligesom databeskyttelsesforordningen ikke indeholder mulighed for, at tilsynsmyndigheden kan træffe afgørelse om tilladelse til behandlingen.

Derudover skal persondatalovens § 7, stk. 7, ses i lyset af databeskyttelsesdirektivets artikel 8, stk. 4. Ordningen i persondatalovens § 7, stk. 7, med, at tilsynsmyndigheden skal give tilladelse til behandlingen, samt at Kommissionen skal underrettes, bliver ikke videreført i forordningen, når den finder anvendelse den 25. maj 2018, idet forordningens artikel 9, stk. 2, litra g, alene kræver, at behandlingen sker på grundlag af EU-retten eller medlemsstaternes nationale ret.

Det fremgår af præambelbetragtning nr. 52, at der også bør gives mulighed for at fravige forbuddet mod at behandle særlige kategorier af personoplysninger, når det er fastsat i EU-retten eller medlemsstaternes nationale ret og er omfattet af de fornødne garantier, således at personoplysninger og andre grundlæggende rettigheder beskyttes, hvis dette er i samfundets interesse, navnlig behandling af personoplysninger inden for ansættelsesret, socialret, herunder pensioner og med henblik på sundhedssikkerhed, overvågning og varsling, forebyggelse eller kontrol af overførbare sygdomme og andre alvorlige trusler mod sundheden.

Det fremgår dernæst af betragtningen, at en sådan fravigelse kan ske til sundhedsformål, herunder folkesundhed og forvaltning af sundhedsydelser, især for at sikre kvaliteten og omkostningseffektiviteten af de procedurer, der anvendes til afregning i forbindelse med ydelser og tjenester inden for sygesikringsordninger, eller til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål.

Det fremgår endvidere af præambelbetragtning nr. 55, at offentlige myndigheders behandling af personoplysninger med henblik på at forfølge officielt anerkendte religiøse sammenslutningers målsætninger, der er fastsat ved forfatningsretten eller ved folkeretten, også foretages i samfundets interesse.

Det fremgår endelig af præambelbetragtning nr. 56, at hvis det i forbindelse med afholdelse af valg i en medlemsstat er nødvendigt, for at det demokratiske system kan fungere, at politiske partier indsamler personoplysninger om enkeltpersoners politiske holdninger, kan behandling af sådanne oplysninger tillades af hensyn til varetagelsen af samfundsinteresser, såfremt fornødne garantier er etableret.

Databeskyttelsesforordningens artikel 9, stk. 2, litra g, giver mulighed for, at der kan ske behandling på grundlag af EU-retten eller medlemsstaternes nationale ret. Der er det yderligere krav, at behandlingen skal være nødvendig at hensyn til væsentlige samfundsinteresser, ligesom lovgivningen skal sikre passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

I forhold til national ret eller EU-ret følger det af forordningens artikel 9, stk. 2, litra g, at lovgivningen skal sikre passende og *specifikke* foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser, i modsætning til eksempelvis artikel 9, stk. 2, litra b, der alene stiller krav om "fornødne garantier". Heri må ligge et krav om, at foranstaltningerne til beskyttelse skal være klare og præcist afgrænsede i forhold beskyttelse af den registrerede grundlæggende rettigheder og interesser. Databeskyttelsesforordningen ses i vidt omfang at indeholde bestemmelser, som specifikt beskytter grundlæggende rettigheder og interesser, men med kravet om specifikke foranstaltninger må lovgiver være opmærksom på så vidt muligt klart og præcist afgrænset at sikre beskyttelsen af den registreredes grundlæggende rettigheder og interesser. Det vil i et lovforslag konkret kunne overvejes at fastsætte yderligere specifikke foranstaltninger, udover rettighederne i databeskyttelsesforordningen, eksempelvis en særlig tavshedspligt eller en særlig begrænsning af, hvilke personer, som har adgang til oplysningerne.

Derudover indeholder bestemmelsen et proportionalitetsprincip, hvorefter lovgivningen skal stå i rimeligt forhold til det mål, der forfølges, og endelig skal lovgivningen respektere det væsentligste indhold af retten til databeskyttelse. Dette proportionalitetsprincip må svare til det proportionalitetsprincip, som følger af databeskyttelsesforordningens artikel 5, stk. 1, litra c.

3.8.3.8. Databeskyttelsesforordningens artikel 9, stk. 2, litra h, og stk. 3

Det fremgår af databeskyttelsesforordningens artikel 9, stk. 2, litra h, at behandling af følsomme oplysninger er lovlig, hvis behandling er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson og underlagt de betingelser og garantier, der er omhandlet i artikel 9, stk. 3.

Databeskyttelsesforordningens artikel 9, stk. 2, litra h, svarer i vidt omfang til bestemmelserne i persondatalovens § 7, stk. 5, og databeskyttelsesdirektivets artikel 8, stk. 3.

Efter artikel 9, stk. 3, kan personoplysninger som omhandlet i stk. 1 behandles til de formål, der er omhandlet i stk. 2, litra h, hvis disse oplysninger behandles af en fagperson, der har tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret eller regler, der er fastsat af nationale kompetente organer, eller under en sådan persons ansvar, eller af en anden person, der også har tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret eller regler, der er fastsat af nationale kompetente organer.

Når det af databeskyttelsesforordningens artikel 9, stk. 3, fremgår, at oplysninger behandles af en fagperson, der har tavshedspligt i henhold til medlemsstaternes nationale ret, må det antages at gælde for den persongruppe, som i dag er omfattet af persondatalovens § 7, stk. 5, det vil sige personer inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt. Dette gælder bl.a. personer omfattet af straffelovens §§ 152 og 152 a-f, og sundhedspersoner, som ifølge sundhedslovens § 40 er undergivet lovbestemt tavshedspligt. Endvidere må det antages at artikel 9, stk. 3, omfatter de almindelige regler om tavshedspligt i forvaltningsloven, herunder tavshedspålæg efter forvaltningslovens § 27, stk. 6.

Databeskyttelsesforordningens artikel 9, stk. 3, ses således også at være en videreførelse af gældende ret, idet behandlingen af personoplysninger efter persondatalovens § 7, stk. 5, også skal ske af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

Som nævnt viderefører bestemmelserne i vidt omfang gældende ret. Imidlertid tilføjes i forordningens artikel 9, stk. 2, litra h, *ydelse og forvaltning af socialomsorg* til formålene, som særlige kategorier af personoplysninger omfattet af stk. 1 kan behandles til, hvis det er nødvendigt herfor. Bestemmelsen må således anses at indebære en udvidelse i forhold til den gældende bestemmelse i persondatalovens § 7, stk. 5, således, at det bliver muligt at behandle følsomme oplysninger, når det er nødvendigt på dele af det sociale område, som ikke anses at være en del af eller have direkte tilknytning til opgaverne på sundhedsområdet.

Det må antages eksempelvis at gælde i forhold til tilbud, der gives efter lov om social service.

Endvidere er *arbejdsmedicin til vurdering af arbejdstagernes erhvervsevne* tilføjet til formålene. Idet der ikke umiddelbart er en direkte forbindelse mellem vurdering af arbejdstagernes erhvervsevne og de formål, der er nævnt i persondatalovens § 7, stk. 5, må databeskyttelsesforordningens artikel 9, stk. 2, litra h, også på dette punkt anses for at være en udvidelse af formålene i forhold til den gældende bestemmelse i persondatalovens § 7, stk. 5.

Det fremgår bl.a. af databeskyttelsesforordningens præambelbetragtning nr. 52, at der bør gives mulighed for at fravige forbuddet mod at behandle særlige kategorier af personoplysninger, når det er fastsat i EU-retten eller medlemsstaternes nationale ret og er omfattet af de fornødne garantier, således at personoplysninger og andre grundlæggende rettigheder beskyttes, hvis dette er i samfundets interesse, navnlig behandling af personoplysninger inden for ansættelsesret, socialret, herunder pensioner og med henblik på sundhedssikkerhed, overvågning og varsling, forebyggelse eller kontrol af overførbare sygdomme og andre alvorlige trusler mod sundheden. Det fremgår endvidere heraf, at fravigelse kan ske til sundhedsformål, herunder folkesundhed og forvaltning af sundhedsydelser, især for at sikre kvaliteten og omkostningseffektiviteten af de procedurer, der anvendes til afregning i forbindelse med ydelser og tjenester inden for sygesikringsordninger, eller til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål.

Derudover følger det af præambelbetragtning nr. 53, at særlige kategorier af personoplysninger, som bør nyde højere beskyttelse, kun bør behandles til sundhedsmæssige formål, når det er nødvendigt for at opfylde disse formål til gavn for fysiske personer og samfundet som helhed, navnlig i forbindelse med forvaltning af sundheds- eller socialydelser og -systemer, herunder administrationens og centrale nationale sundhedsmyndigheders behandling af sådanne oplysninger med henblik på kvalitetskontrol, ledelsesinformation og det generelle nationale og lokale tilsyn med sundheds- eller socialsystemet, og for at sikre kontinuitet inden for sundheds- eller socialforsorg og sundhedsydelser på tværs af grænserne eller med henblik på sundhedssikkerhed, overvågning og varsling eller til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål baseret på EU-retten eller medlemsstaternes nationale ret, og som skal opfylde et formål af offentlig interesse, samt studier, der foretages i samfundets interesse på folkesundhedsområdet. Endvidere følger det heraf, at forordningen derfor bør fastsætte harmoniserede betingelser for behandling af særlige kategorier af personoplysninger om helbredsforhold for så vidt angår specifikke behov, navnlig hvis behandlingen af sådanne oplysninger foretages til visse sundhedsmæssige formål af personer, der er underlagt tavshedspligt.

Persondataloven indeholder som anført i § 7, stk. 5, en bestemmelse om, at følsomme oplysninger kan behandles på sundhedsområdet. Bestemmelsen bygger på databeskyttelsesdirektivets artikel 8, stk. 3, der svarer til databeskyttelsesforordningens artikel 9, stk. 2, litra h. Som et eksempel vil persondatalovens § 7, stk. 5, således kunne opretholdes efter den 25. maj 2018, hvorfra forordningen skal anvendes.

3.8.3.9. Databeskyttelsesforordningens artikel 9, stk. 2, litra i

Det fremgår af databeskyttelsesforordningens artikel 9, stk. 2, litra i, at behandling af følsomme oplysninger er lovlig, hvis behandling er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, f.eks. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitets- og sikkerhedsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr på grundlag af EU-retten eller medlemsstaternes nationale ret, som fastsætter passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder, navnlig tavshedspligt.

Databeskyttelsesforordningens artikel 9, stk. 2, litra i, knytter sig, som databeskyttelsesforordningens artikel 9, stk. 2, litra g, til databeskyttelsesdirektivets artikel 8, stk. 4, hvorefter medlemsstaterne kan fastsætte andre undtagelser af grunde, der vedrører hensynet til vigtige samfundsinteresser.

Det fremgår af præambelbetragtning nr. 53, at særlige kategorier af personoplysninger, som bør nyde højere beskyttelse, bl.a. kun bør behandles til studier, der foretages i samfundets interesse på folkesundhedsområdet.

Det fremgår endvidere af præambelbetragtning nr. 54, at behandling af særlige kategorier af personoplysninger kan være nødvendig af hensyn til samfundsinteresser hvad angår folkesundhed uden den registreredes samtykke. En sådan behandling bør være underlagt passende og specifikke foranstaltninger med henblik på at beskytte fysiske personers rettigheder og frihedsrettigheder. I denne sammenhæng fortolkes »folkesundhed« som defineret i Europa-Parlamentets og Rådets forordning (EF) nr. 1338/2008 (11), dvs. alle elementer vedrørende sundhed, nemlig helbredstilstand, herunder sygelighed og invaliditet, determinanter med en indvirkning på helbredstilstanden, behov for sundhedspleje, ressourcer tildelt sundhedsplejen, ydelse af og almen adgang til sundhedspleje, udgifter til og finansiering af sundhedspleje samt dødsårsager. Sådan behandling af helbredsoplysninger af hensyn til samfundsinteresser bør ikke medføre, at tredjemænd såsom arbejdsgivere eller forsikringsselskaber og pengeinstitutter, behandler personoplysninger til andre formål.

Databeskyttelsesforordningens artikel 9, stk. 2, litra i, giver mulighed for, at der kan ske behandling på grundlag af EU-retten eller medlemsstaternes nationale ret. Der er det yderligere krav, at behandlingen skal være nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, ligesom lovgivningen skal sikre passende og specifikke foranstaltningen til beskyttelse af den registreredes grundlæggende rettigheder og frihedsrettigheder, navnlig tavshedspligt.

I forhold til national ret eller EU-ret følger det af forordningens artikel 9, stk. 2, litra i, at lovgivningen skal sikre passende og *specifikke* foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser, navnlig tavshedspligt. Heri må ligge et krav om, at foranstaltningerne til beskyttelse skal være klare og præcist afgrænsede i forhold til beskyttelse af den registreredes grundlæggende rettigheder og interesser. Databeskyttelsesforordningen ses i vidt omfang at indeholde bestemmelser, som specifikt beskytter grundlæggende rettigheder og interesser, men med kravet om specifikke foranstaltninger må lovgiver være opmærksom på så vidt muligt klart og præcist afgrænset at sikre beskyttelsen af den registreredes grundlæggende rettigheder og interesser. Da tavshedspligt særligt er fremhævet, vil man specifikt skulle være opmærksom herpå.

3.8.3.10. Databeskyttelsesforordningens artikel 9, stk. 2, litra j

Det fremgår af databeskyttelsesforordningens artikel 9, stk. 2, litra j, at behandling af følsomme oplysninger er lovlig, hvis behandling er nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Databeskyttelsesforordningens artikel 9, stk. 2, litra j, knytter sig, som databeskyttelsesforordningens artikel 9, stk. 2, litra g, til databeskyttelsesdirektivets artikel 8, stk. 4, hvorefter medlemsstaterne kan fastsætte andre undtagelser af grunde, der vedrører hensynet til vigtige samfundsinteresser.

Det fremgår af præambelbetragtning nr. 53, at særlige kategorier af personoplysninger, som bør nyde højere beskyttelse, bl.a. kun bør behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål baseret på EU-retten eller medlemsstaternes nationale ret, og som skal opfylde et formål af offentlig interesse.

Databeskyttelsesforordningens artikel 9, stk. 2, litra j, giver mulighed for, at der kan ske behandling på grundlag af EU-retten eller medlemsstaternes nationale ret. Det er et krav, at behandlingen skal være nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, ligesom lovgivningen skal sikre passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

I forhold til national ret eller EU-ret følger det af forordningens artikel 9, stk. 2, litra j, at lovgivningen skal sikre passende og *specifikke* foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser. Heri må ligge et krav om, at foranstaltningerne til beskyttelse skal være klare og præcist afgrænsede i forhold beskyttelse af den registrerede grundlæggende rettigheder og interesser. Databeskyttelsesforordningen ses i vidt omfang at indeholde bestemmelser, som specifikt beskytter grundlæggende rettigheder og interesser, men med kravet om specifikke foranstaltninger må man være opmærksom på så vidt muligt klart og præcist afgrænset at sikre beskyttelsen af den registreredes grundlæggende rettigheder og interesser.

Derudover indeholder bestemmelsen et proportionalitetsprincip, hvorefter lovgivningen skal stå i rimeligt forhold til det mål, der forfølges, og endelig skal lovgivningen respektere det væsentligste indhold af retten til databeskyttelse. Dette proportionalitetsprincip må svare til det proportionalitetsprincip, som følger af databeskyttelsesforordningens artikel 5, stk. 1, litra c.

For nærmere om databeskyttelsesforordningens artikel 89, stk. 1, henvises til afsnit 10.5. og 10.6. om artikel 89.

3.8.3.10. Nationalt råderum i databeskyttelsesforordningens artikel 9, stk. 2, litra b, g, h, i og j

Vedrørende muligheden for at vedtage national lovgivning følger det af præambeltragtning nr. 10, at forordningen også indeholder en manøvremargen, så medlemsstaterne kan præcisere reglerne heri, herunder for behandling af følsomme oplysninger omfattet af artikel 9. Det fremgår også af præambelbetragtningen, at forordningen således ikke udelukker, at medlemsstaterne i sin nationale lovgivning fastlægger eller opretholder regler om de nærmere omstændigheder for de specifikke databehandlingssituationer, herunder mere præcis fastlæggelse af de forhold, hvorunder behandling af personoplysninger er lovlig.

Som nævnt ovenfor synes artikel 9, stk. 2, litra b, g, h, i og j med henvisningerne til EU-retten eller medlemsstaternes nationale ret, at forudsætte, at behandlingen er forankret i f.eks. national ret for, at udgangspunktet i artikel 9, stk. 1, om forbud mod behandling af følsomme oplysninger, kan fraviges.

Databeskyttelsesforordningens artikel 9, stk. 2, litra b, g, h, i og j, kræver således en udfyldning i EU-retten eller national ret og vil ikke uden videre kunne anvendes som direkte behandlingshjemmel.

Som fortolkningsbidrag hertil fremgår det af præambelbetragtning nr. 41, at når denne forordning henviser til et retsgrundlag eller en lovgivningsmæssig foranstaltning, kræver det ikke nødvendigvis en lov, der er vedtaget af et parlament, med forbehold for krav i henhold til den forfatningsmæssige orden i den pågældende medlemsstat.

Retsgrundlaget kan således også fremgå af en bekendtgørelse. Et sådant retsgrundlag eller en sådan lovgivningsmæssig foranstaltning skal imidlertid efter præambelbetragtningen være klar(t) og præcis(t), og anvendelse heraf bør være forudsigelig for personer, der er omfattet af dets/dens anvendelsesområde, jf. retspraksis fra EU-Domstolen og Den Europæiske Menneskerettighedsdomstol.

Internationale forpligtelser antages også at falde ind under medlemsstaternes nationale ret, idet internationale forpligtelser må anses som værende blevet en del af en medlemsstats nationale ret efter det enkelte lands forskellige tiltrædelsesregler. Endvidere kan der henvises til, at der i afsnit 3.3. om lovlig behandling af ikke-følsomme oplysninger, artikel 6, stk. 1, omkring litra c anføres, at en retlig forpligtelse også vil være forpligtelser, der følger af internationale regler.

Artikel 9, stk. 2, litra b, g, h, i og j, skal på den baggrund anses for både at være udtryk for et nationalt råderum til at vedtage regler om behandling af personoplysninger på de pågældende litraers områder, men også således, at de pågældende regler skal "aktiveres" i national ret (eller i andre EU-retsakter) for, at forbuddet i artikel 9, stk. 1, kan anses for fraveget. Artikel 9, stk. 2, litra h, kan aktiveres "i henhold til en kontrakt med en sundhedsperson", jf. bestemmelsens ordlyd.

Det må i den forbindelse antages, at der ikke er noget til hinder for, at forordningens artikel 9, stk. 2, litra b, g, h, i og j, gennemføres som behandlingsregler på *generel vis* i en kommende udgave af persondataloven ved en nærmest ordret implementering – på samme måde som med f.eks. persondatalovens § 7, stk. 7, der er en tekstnær implementering af databeskyttelsesdirektivets artikel 8, stk. 4.

Dette underbygges af præambelbetragtning nr. 8, hvoraf det fremgår, at når forordningen fastsætter, at der kan indføres specifikationer eller begrænsninger af dens regler ved medlemsstaternes nationale ret, kan medlemsstaterne, i det omfang det er nødvendigt af hensyn til sammenhængen og for at gøre de nationale bestemmelser forståelige for de personer, som de finder anvendelse på, indarbejde elementer af denne forordning i deres nationale ret.

Artikel 9, stk. 2, litra b, g, h, i og j, kan også *aktiveres* via national *særlovgivning*. Det må i den forbindelse antages at være tilstrækkeligt, at den pågældende behandling af personoplysninger er forudsat i særlovgivningen. Det kan således ikke være et krav, at den pågældende særlovgivning indeholder en udtrykkelig regel om *behandlingen* af personoplysninger i forbindelse med brug af f.eks. artikel 9, stk. 2, litra g, om "væsentlige samfundsinteresser".

Formuleringen af artikel 9, stk. 2, litra b, g, h, i og j, må i den forbindelse også forstås således, at man nationalt kan beslutte alene at aktivere de forskellige litraer som hjemmelsgrundlag *i et vist omfang*. Eksempelvis omhandler artikel 9, stk. 2, litra b, "arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder". I og med at litra b, g, h, i og j ikke kan anvendes uden videre som direkte behandlingsgrundlag må medlemsstaterne lovgivningsmæssig kunne bestemme, at alene en del heraf skal kunne anvendes – i litra b's tilfælde, f.eks. alene for så vidt angår "arbejdsretlige forpligtelser". I det omfang medlemsstaterne ikke har valgt at aktivere hele eller dele af de pågældende bestemmelser i sin lovgivning, falder man tilbage på forbuddet i artikel 9, stk. 1, mod at behandle de pågældende følsomme personoplysninger.

Det fremgår i øvrigt af databeskyttelsesforordningens artikel 9, stk. 2, litra b, g, h, i og j, at lovgiver – i forbindelse med udnyttelse af råderummet i de pågældende litraer – skal iagttage visse krav som nærmere beskrevet i bestemmelserne, eksempelvis skal der efter artikel 9, stk. 2, litra g, fastsættes passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder.

Sådanne krav om fastsættelse af passende og specifikke foranstaltninger bevirker, at det i forbindelse med udarbejdelse af den nationale lov skal vurderes, hvilke foranstaltninger, der kan fastsættes udover de foranstaltninger, som allerede følger af forordningen. I den forbindelse må det kunne fastsættes, at den dataansvarlige pålægges pligten til at sikre passende og specifikke foranstaltninger. Endvidere er parterne i en overenskomst forpligtede til at iagttage de fornødne garantier, og parterne har således ansvaret herfor, når der fastsættes bestemmelser efter forordningens artikel 9, stk. 2, litra b.

Som inspiration til, hvad der kan være passende og specifikke foranstaltninger, kan der som eksempel skeles til, hvad Registerudvalget i betænkning nr. 1345 fandt, var *tilstrækkelige garantier*. Registerudvalget anførte således, at der var tale om tilstrækkelige garantier i forbindelse med indførelsen af persondatalovens § 9, vedtaget indenfor rammerne af databeskyttelsesdirektivets artikel 8, stk. 4, om retsinformationssystemer, når det blev indført, at tilsynsmyndigheden kunne fastsætte nærmere vilkår for behandlinger, og når der blev stillet vilkår om, at personnavne, præcise adresseangivelser og eventuelt andre identifikati-

onsoplysninger fjernes, herunder vilkår om, at der ikke måtte kunne søges på navne mv., i det omfang der ikke skete anonymisering. Særligt i forbindelse med retsinformationssystemer fandt Registerudvalget, at der var tale om tilstrækkelige garantier, når det i loven blev fastsat, at oplysninger, som behandledes ikke senere måtte behandles i andet øjemed.[269]

Databeskyttelsesforordningens generelle formål, ordlyden i forordningens artikel 9, stk. 2, litra b, g, h, i og j, samt de ovenfor nævnte præambelbetragtninger indikerer ikke, at det har været hensigten med disse bestemmelser, at der med databeskyttelsesforordningen er tiltænkt et andet rum end efter direktivet for at fastsætte nationale regler i forbindelse med behandling af følsomme oplysninger.

For særlovgivningen og de gældende overenskomster vil dette betyde, at medlemsstaterne kan *opretholde* nationale bestemmelser, som blev vurderet som værende i overensstemmelse med databeskyttelsesdirektivet – eksempelvis artikel 8, stk. 4 – idet hjemlen nu fremover vil være i databeskyttelsesforordningens artikel 9, stk. 2, litra b, g, h, i eller j – forudsat at kravene i de forskellige litraer er iagttaget, eksempelvis kravet om passende og specifikke foranstaltninger.

Det må således normalt antages, at den nationale særlovgivning, som er fastsat i overensstemmelse med direktivet, allerede opfylder kravene i forordningens artikel 9, stk. 2, litra b, g, h, i eller j, om blandt andet passende og specifikke foranstaltninger, idet lovgivningen allerede efter databeskyttelsesdirektivet bl.a. skulle give tilstrækkelige garantier.

Det må på den baggrund antages, at eksisterende nationale særregler om eksempelvis indsamling, videregivelse, samkøring eller sletning mv., jf. forordningens artikel 4, nr. 2, der definerer behandling, vil kunne bestå.

Der må endvidere antages, at der er adgang til at opretholde konkrete lovregler om eksempelvis behandling af følsomme oplysninger i sundhedssektoren.

Muligheden for at opretholde eller indføre yderligere betingelser, herunder begrænsninger, er dog begrænset af, at det ikke bør hæmme den frie udveksling af personoplysninger i EU, når disse betingelser finder anvendelse på grænseoverskridende behandling af sådanne oplysninger. Dette krav må i praksis navnlig antages at have relevans for regulering, der direkte er rettet mod den private sektor eller i væsentlig grad påvirker denne, idet hensynet til den fri bevægelighed må antages i praksis at have mere begrænset betydning for den

[269] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 252.

offentlige sektor. Dog vil ethvert relevant lovgivningsmæssigt tiltag mv. skulle vurderes i forhold til dette krav, uanset om det er rettet mod den private eller offentlige sektor.

3.8.4. Overvejelser

Databeskyttelsesforordningens artikel 9, stk. 2, litra a, c, e og f er udtryk for en videreførelse af gældende ret.

Vedrørende databeskyttelsesforordningens artikel 9, stk. 2, litra b, indeholder databeskyttelsesdirektivet i artikel 8, stk. 2, litra b, en delvist tilsvarende bestemmelse. Efter databeskyttelsesforordningens artikel 9, stk. 2, litra b, ses der i forbindelse med arbejdsretlige forpligtelser således at være samme mulighed for behandling på grundlag af EU-retten eller medlemsstaternes nationale ret eller en kollektiv overenskomst som efter gældende ret. Bestemmelsen i forordningens artikel 9, stk. 2, litra b, omfatter som nævnt også sundheds- og socialretlige forpligtelser. For særlovgivningen og de gældende overenskomster i medfør af medlemsstaternes nationale ret vil dette betyde, at medlemsstaterne vil kunne opretholde disse under den forudsætning, at særlovgivningen og overenskomsterne opfylder kravene i forordningens artikel 9, stk. 2, litra b.

Databeskyttelsesforordningens artikel 9, stk. 2, litra d, ses ikke at være en ændring af gældende ret – dog vil bestemmelsen efter forordningens virkning nu også vedrøre tidligere medlemmer modsat, hvad der følger af gældende ret.

Databeskyttelsesforordningens artikel 9, stk. 2, litra g, svarer efter ordlyden delvist til databeskyttelsesdirektivets artikel 8, stk. 4, og databeskyttelsesforordningens artikel 9, stk. 2, litra i og j, knytter sig til databeskyttelsesdirektivets artikel 8, stk. 4, men der er ikke en tilsvarende bestemmelse i persondataloven. Det antages, at der er samme mulighed for behandling på grundlag af EU-retten eller medlemsstaternes nationale ret efter artikel 9, stk. 2, litra g, i og j, som efter gældende ret.

Lovgiver vil dog skulle være opmærksom på, at de særlige krav, som fastsættes i forordningen vil skulle iagttages, når der fastsættes lovgivning. For særlovgivningen vil dette betyde, at medlemsstaterne vil kunne opretholde særlovgivning under den forudsætning, at særlovgivningen opfylder de øvrige tilføjede krav til lovgivningen, som fremgår af forordningens artikel 9, stk. 2, litra g, i og j.

Databeskyttelsesforordnings artikel 9, stk. 2, litra h, ses at være i overensstemmelse med, hvad der følger af gældende ret – dog er der de ovennævnte tilføjelser om *ydelse og forvaltning af socialomsorg* samt *arbejdsmedicin til vurdering af arbejdstagernes erhvervsevne*, der således er en udvidelse af anvendelsesområdet i forhold til gældende ret.

Databeskyttelsesforordningens artikel 9, stk. 3, ses også at være i overensstemmelse med, hvad der følger af gældende ret, idet bestemmelsen dog indeholder en mere detaljeret regulering af, hvad der gælder efter forordningens artikel 9, stk. 2, litra h.

3.8.4.1. "Tjekliste" for bedømmelse af eksisterende nationale særregler vedrørende følsomme oplysninger om behandlings forenelighed med databeskyttelsesforordningen
Denne tjekliste vedrører muligheden for at opretholde regler for lovlig behandling i overensstemmelse med artikel 9. Tjeklisten medtager således ikke andre og mere specifikke krav, som den nationale lovgiver også skal være opmærksom på, som eksempelvis den registreredes rettigheder og begrænsninger heraf, jf. artikel 23, artikel 26 om fælles dataansvarlige og artikel 28 om databehandler. For nærmere herom henvises bl.a. til afsnit 4.13. om begrænsninger af rettigheder, artikel 23.

Når myndigheder skal overveje, hvorvidt eksisterende nationale særregler kan opretholdes, når databeskyttelsesforordningen finder anvendelse, anbefales følgende punkter sammenfattende iagttaget i forhold til vurderingen af, om der er hjemmel til behandlingen:

Det skal bemærkes, at det må antages, at eksisterende nationale særregler om behandling, som tidligere anført, i langt de fleste tilfælde vil kunne bestå.

1. Det kan indledningsvis overvejes, om den nationale regel fortsat ønskes opretholdt, eller hvorvidt behandling fremover skal ske alene efter behandlingsreglerne i databeskyttelsesforordningen, eksempelvis forordningens artikel 9, stk. 2, litra f, om behandling, der er nødvendig, for at retskrav kan fastlægges, der kan anvendes direkte som behandlingshjemmel.

I den forbindelse kan det indgå i vurderingen, om retsområdet kan administreres alene og direkte på grundlag af behandlingsreglerne i forordningen, hvilket er tilfældet med artikel 9, stk. 2, litra a, c, d, e og f, hvorimod artikel 9, stk. 2, litra b, g, h, i og j, kræver udfyldning i særlovgivningen.

I det omfang det foreslås at opretholde nationale særregler, der har erhvervsøkonomiske konsekvenser for danske virksomheder, skal der tages stilling til, om principperne for implementering af erhvervsrettet EU-regulering i Danmark efterleves. Hvis principperne ikke efterleves, og den opretholdte regel indgår i et forslag til en ny lov eller bekendtgørelse, skal der forelægges en sag for Implementeringsudvalget.[270]

[270] Se nærmere på Beskæftigelsesministeriets hjemmeside.

2. Dernæst bør det vurderes, hvorvidt hjemlen til den eksisterende regel kan findes i forordningens artikel 9, stk. 2, litra b, g, h, i eller j.

Det bemærkes, at forordningens artikel 9, stk. 4, endvidere giver medlemsstaterne mulighed for at opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger. For nærmere herom henvises til afsnit 3.9. om medlemsstaternes råderum (ved behandling af følsomme oplysninger), artikel 9, stk. 4, nedenfor.

3. Endvidere skal det iagttages, at særreglen overholder de øvrige krav, som følger af bestemmelserne i artikel 9, stk. 2 og 3, eksempelvis at der fastsættes passende og i visse tilfælde specifikke foranstaltninger samt i nogle tilfælde et særligt krav om, at særreglen er proportional (eksempelvis litra g "står i rimeligt forhold til det mål, der forfølges"). Herunder også reglerne i forordningens artikel 88 og 89.

Samtidig skal reglen overholde principperne for behandling i forordningens artikel 5, hvilket eksempelvis betyder, at lovgivningen ikke må medføre, at der sker en ophobning af data i strid med artikel 5, stk. 1, litra e.

4. Endelig skal det sikres, at der er den rette balance i forhold til den fri bevægelighed for personoplysninger, jf. forordningens artikel 1.

3.8.4.2. "Tjekliste" for udarbejdelse af nye nationale særregler for behandling af følsomme personoplysninger

Denne tjekliste vedrører muligheden for at fastsætte regler for lovlig behandling i overensstemmelse med artikel 9. Tjeklisten medtager således ikke andre og mere specifikke krav, som den nationale lovgiver også skal være opmærksom på, som eksempelvis den registreredes rettigheder og begrænsninger heraf, jf. artikel 23, artikel 26 om fælles dataansvarlige og artikel 28 om databehandler.

Når myndigheder overvejer at udfærdige nationale særregler efter det nationale råderum, som databeskyttelsesforordningen efterlader i artikel 9, stk. 2, litra b, g, h, i og j, anbefales følgende punkter sammenfattende iagttaget i forhold til vurderingen af, om der er hjemmel til behandlingen:

1. Det kan indledningsvis overvejes, om der overhovedet ønskes fastsat en national regel, eller om behandling fremover skal ske alene efter behandlingsreglerne i databeskyttelsesforordningen, eksempelvis forordningens artikel 9, stk. 2, litra f, om behandling, der er

nødvendig, for at retskrav kan fastlægges, der kan anvendes direkte som behandlingshjemmel.

I den forbindelse kan det indgå i vurderingen, om retsområdet kan administreres alene og direkte på grundlag af behandlingsreglerne i forordningen, hvilket er tilfældet med artikel 9, stk. 2, litra a, c, d, e og f, hvorimod artikel 9, stk. 2, litra b, g, h, i og j, kræver udfyldning i særlovgivningen.

I det omfang det foreslås at indføre nationale særregler, der har erhvervsøkonomiske konsekvenser for danske virksomheder, skal der tages stilling til, om principperne for implementering af erhvervsrettet EU-regulering i Danmark efterleves. Hvis principperne ikke efterleves, skal der forelægges en sag for Implementeringsudvalget.[271]

2. Dernæst bør det vurderes, hvorvidt hjemlen til reglen kan findes i forordningens artikel 9, stk. 2, litra b, g, h, i eller j.

Det bemærkes, at forordningens artikel 9, stk. 4, endvidere giver medlemsstaterne mulighed for at opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger. For nærmere herom henvises til afsnit 3.9. om medlemsstaternes råderum (ved behandling af følsomme oplysninger), artikel 9, stk. 4, nedenfor.

3. Endvidere skal det iagttages, at reglen overholder de øvrige krav, som følger af bestemmelserne i artikel 9, stk. 2-3, eksempelvis at der fastsættes passende og i visse tilfælde specifikke foranstaltninger samt i nogle tilfælde et særligt krav om, at særreglen er proportional (eksempelvis litra g "står i rimeligt forhold til det mål, der forfølges"), herunder også reglerne i forordningens artikel 88 og 89.

Samtidig skal reglen overholde principperne for behandling i forordningens artikel 5, hvilket eksempelvis betyder, at lovgivningen ikke må medføre, at der sker en ophobning af data i strid med artikel 5, stk. 1, litra e.

4. Endelig skal det sikres, at der er den rette balance i forhold til den fri bevægelighed for personoplysninger, jf. forordningens artikel 1.

[271] Se nærmere på Beskæftigelsesministeriets hjemmeside.

3.9. Medlemsstaternes råderum (ved behandling af følsomme oplysninger), artikel 9, stk. 4

3.9.1. Præsentation

Databeskyttelsesforordningens artikel 9, stk. 4, indeholder en særlig regel, hvorefter medlemsstaterne kan opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetisk data, biometrisk data eller helbredsoplysninger.

Denne bestemmelse fastsætter grænserne for medlemsstaternes nationale råderum til fastsættelse af nationale særregler for den i bestemmelsen oplistede kategori af oplysninger.

3.9.2. Gældende ret

I databeskyttelsesdirektivet samt i persondataloven er der ikke en bestemmelse, som svarer til databeskyttelsesforordningens artikel 9, stk. 4.

Databeskyttelsesdirektivets artikel 5 regulerer, at medlemsstaterne i henhold til bestemmelserne i kapitel II, vedrørende almindelige betingelser for lovlig behandling af personoplysninger, præciserer, på hvilke betingelser behandling af personoplysninger er lovlig.

I vurderingen af medlemsstaternes mulighed for at fastsætte særregler efter databeskyttelsesdirektivet skal der lægges vægt på databeskyttelsesdirektivets artikel 5, ligesom præambelbetragtningerne nr. 9, 22 og 30 er relevante. Derudover er der også praksis fra EU-Domstolen, som er relevant for vurderingen. For nærmere herom kan henvises til afsnit 3.4. om lovlig behandling af ikke-følsomme oplysninger – nationalt råderum, artikel 6, stk. 2-3.

3.9.3. Databeskyttelsesforordningen

Det fremgår af databeskyttelsesforordningens artikel 9, stk. 4, at medlemsstaterne kan opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger.

Det fremgår af præambelbetragtning nr. 53, at medlemsstaterne bør kunne opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger. Dette bør dog ikke hæmme den frie udveksling af personoplysninger i Unionen, når disse betingelser finder anvendelse på grænseoverskridende behandling af sådanne oplysninger.

Med databeskyttelsesforordningens artikel 9, stk. 4, fremhæves det, at der er et videre rum for nationale regler, for så vidt angår disse særligt oplistede personoplysninger.

Efter databeskyttelsesforordningens artikel 9, stk. 4, ses der således at være en relativt stor manøvremargin for medlemsstaterne til at opretholde eller indføre yderligere betingelser, herunder begrænsninger.

Med *betingelser* må der i denne sammenhæng forstås såvel, at medlemsstaterne nationalt kan fastsætte yderligere krav til, hvornår en behandling er lovlig og til, hvilke foranstaltninger der skal iagttages som led i en given behandling. En medlemsstat vil således – inden for bestemmelsens rammer – have adgang til f.eks. at fastsætte, at en behandling af helbredsoplysninger skal ske på en særlig måde (f.eks. elektronisk), omfatte særlige oplysninger (f.eks. diagnose og sygdomshistorik) og indebære videregivelse til nærmere fastsatte modtagere.

Muligheden for at opretholde eller indføre yderligere betingelser, herunder begrænsninger, er dog begrænset af, at det ikke bør hæmme den frie udveksling af personoplysninger i EU, når disse betingelser finder anvendelse på grænseoverskridende behandling af sådanne oplysninger. Dette krav må i praksis navnlig antages at have relevans for regulering, der direkte er rettet mod den private sektor, eller i væsentlig grad påvirker denne, idet hensynet til den fri bevægelighed må antages i praksis at have mere begrænset betydning for den offentlige sektor. Dog vil ethvert relevant lovgivningsmæssigt tiltag mv. skulle vurderes i forhold til dette krav, uanset om det er rettet mod den private eller offentlige sektor.

Dette krav ses netop at underbygge, at medlemsstaterne – udover ved grænseoverskridende behandling – har et ganske vidt spillerum for at fastsætte nationale særregler.

Muligheden for særregler for lovlig behandling udelukkende med hjemmel i én af behandlingshjemlerne, eksempelvis samtykke
I forbindelse med medlemsstaternes manøvremargin efter databeskyttelsesforordningens artikel 9, stk. 4, kan der opstå den situation, at en medlemsstat ønsker at vedtage en særlovgivning, hvor en behandling kun vil være lovlig efter én bestemt behandlingshjemmel, eksempelvis såfremt den registrerede har givet sit udtrykkelige samtykke til behandlingen.

I sådanne situationer udelukker særloven altså, at de andre behandlingshjemler end et samtykke kan finde anvendelse.

Efter databeskyttelsesforordningens artikel 9, stk. 4, vil det vedrørende genetisk data, biometrisk data og helbredsoplysninger være muligt bl.a. at opretholde eller indføre begrænsninger, jf. ordene "herunder begrænsninger" i artikel 9, stk. 4.

Vedrørende behandling af genetisk data, biometrisk data og helbredsoplysninger, antages det derfor at være muligt at opretholde eller indføre regler om, at behandling af oplysninger i forbindelse med en operation eksempelvis altid kræver samtykke som hjemmel, og således ikke kan ske med hjemmel i de andre behandlingshjemler i artikel 9.

Når man på den baggrund nationalt fastlægger, at en bestemt behandling alene kan ske på baggrund af samtykke, bør samtykket – i overensstemmelse med retningen i ASNEF-dommen, som er omtalt i afsnit 3.4. om lovlig behandling af ikke-følsomme oplysninger – nationalt råderum, artikel 6, stk. 2-3 – være i overensstemmelse med samtykket i forordningen, som nærmere beskrives i artikel 4, nr. 11 og artikel 7.

3.9.4. Overvejelser

Efter databeskyttelsesforordningens artikel 9, stk. 4, overlades medlemsstaterne et betydeligt råderum til at fastsætte nationale særregler for at opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetisk data, biometrisk data eller helbredsoplysninger.

3.10. Strafbare forhold, herunder straffe- og børneattester, artikel 10, 1. pkt.

3.10.1. Præsentation

I persondatalovens § 8 er der fastsat betingelser for, hvornår offentlige og private kan behandle oplysninger om strafbare forhold, herunder oplysninger om straffe- og børneattester. Bestemmelsen er baseret på artikel 8, stk. 5, i databeskyttelsesdirektivet, hvorefter det kun er offentlige myndigheder, der kan behandle sådanne oplysninger. Private kan derimod kun behandle oplysninger om lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger, hvis der gælder tilstrækkelige, specifikke garantier i medfør af national ret.

Databeskyttelsesforordningen indeholder en tilsvarende bestemmelse i artikel 10, 1. pkt., hvorefter det som udgangspunkt kun er offentlige myndigheder, der kan behandle personoplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på baggrund af forordningens artikel 6, stk. 1. Private kan kun foretage behandling af disse oplysninger på baggrund af EU-ret eller medlemsstaternes nationale ret, hvis der gives passende garantier for registreredes rettigheder og frihedsrettigheder.

3.10.2. Gældende ret

3.10.2.1. Databeskyttelsesdirektivets artikel 8, stk. 5

Databeskyttelsesdirektivets artikel 8, stk. 5, 1. afsnit, fastsætter, at oplysninger om lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger tilhører en særlig kategori af oplysninger.[272] Det fremgår endvidere af bestemmelsen, at behandling af sådanne oplysninger som udgangspunkt kun må foretages under kontrol af en offentlig myndighed.

Hvis der gælder tilstrækkelige, specifikke garantier i medfør af den nationale lovgivning, herunder administrative forskrifter fastsat i henhold til lov, kan behandling af sådanne oplysninger dog også udføres for private. Såfremt der er tale om et fuldstændigt register over straffedomme, skal dette dog altid føres under kontrol af en offentlig myndighed, jf. artikel 8, stk. 5, 2. pkt.

Registerudvalget anførte i betænkning nr. 1345, at der ikke i direktivet er taget stilling til, hvad der skal forstås ved udtrykket *oplysninger om lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger*.[273] Registerudvalget anførte dog, at udtrykkene formentlig må anses for at være dækket af udtrykket "strafbare forhold" som efter den hidtil gældende registerlovgivning. På denne baggrund – og idet det blev forudsat, at udtrykket "strafbare forhold" fortolkes i lyset af direktivets artikel 8, stk. 5 – fandt Registerudvalget, at dette udtryk skulle anvendes i forbindelse med udformning af de materielle danske regler for behandling af sådanne oplysninger.

For så vidt angik direktivets artikel 8, stk. 5, *1. afsnit*, anførte Registerudvalget, at der ikke i bestemmelsen fastsættes regler for, hvilke materielle behandlingskriterier, der skal gælde for behandling af oplysninger om strafbare forhold.

Registerudvalget bemærkede hertil, at oplysninger om strafbare forhold ikke er nævnt i artikel 8, stk. 1, som er den bestemmelse i direktivet, der indeholder kategorier af følsomme oplysninger. I stedet er oplysninger om strafbare forhold nævnt i den selvstændige bestemmelse i artikel 8, stk. 5. Denne opbygning måtte – ifølge Registerudvalget – antages at indebære, at oplysninger om strafbare forhold ikke er omfattet af reguleringen i bestemmelserne i artikel 8, stk. 2-4, som udgør de materielle behandlingskriterier for følsomme oplysninger.

I stedet antog Registerudvalget, at direktivet bygger på den ordning, at spørgsmålet, om hvorvidt behandling af oplysninger om strafbare forhold lovligt kan ske, skal afgøres under

[272] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 241.
[273] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 241.

hensynstagen til de principper vedrørende grundlaget for behandling af oplysninger, som indeholdt i direktivets artikel 7.

På denne baggrund fandt Registerudvalget[274], at der i dansk lovgivning burde fastsættes særlige regler om, hvornår behandling af oplysninger om strafbare forhold kan finde sted. Registerudvalget bemærkede i den forbindelse, at der i medfør af direktivet er overladt et vist spillerum for medlemsstaterne til at fastlægge de nærmere kriterier for adgangen til at behandle oplysninger, der ikke – i direktivets forstand – har karakter af særlige følsomme oplysninger, jf. præambelbetragtning nr. 22 i direktivet.[275]

Det fremgår endvidere af bemærkningerne til persondataloven, at persondatalovens § 8 har til formål at udgøre en del af den samlede danske gennemførelse af direktivets – mindre restriktive – regler for behandling af andre typer personoplysninger, jf. direktivets artikel 7.[276]

Registerudvalget anførte endvidere i betænkning nr. 1345[277], at der i udformningen af de danske regler om behandling af oplysninger om strafbare forhold efter udvalgets opfattelse burde sondres mellem behandling, som udføres for henholdsvis offentlige myndigheder og private.

Som følge heraf, og i lyset af direktivets artikel 8, stk. 5, er der således i dansk ret fastlagt særlige regler for behandling af oplysninger om bl.a. strafbare forhold for henholdsvis offentlige myndigheder og private i persondatalovens § 8.

3.10.2.2. Oplysninger om strafbare forhold

Efter praksis skal der anlægges en ganske vid forståelse af begrebet strafbare forhold omfattet af persondatalovens § 8, *stk. 1*. Det følger således af praksis, at ikke blot oplysninger om overtrædelse af lovgivning, uden at det har udløst eller kan udløse et egentligt strafansvar, men eventuelt andre sanktioner, som f.eks. rettighedsfrakendelse, antagelig må anses for omfattet af persondatalovens § 8.[278]

Det er imidlertid ikke enhver oplysning om et muligt strafbart forhold, herunder om enhver anmeldelse til politiet, der kan anses for omfattet af persondatalovens § 8, *stk. 1*. Hertil

[274] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 242.
[275] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 242.
[276] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 8.
[277] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 242.
[278] Persondataloven med kommentarer (2015), s. 310-311.

kræves, at anmeldelsen til politiet i en eller anden form må antages at være underbygget, førend der er tale om oplysninger om strafbare forhold.

På den ene side vil f.eks. en oplysning, som indgår i en sag hos en forvaltningsmyndighed om, at en fysisk person har været udsat for chikane eller grundløs politianmeldelse, f.eks. fra en anden borger, næppe være omfattet af persondatalovens § 8. På den anden side må en oplysning om, at en forvaltningsmyndighed efter grundig undersøgelse af en sag inden for myndighedens ressortområde er nået til den konklusion, at en fysisk person må antages at have overtrådt lovgivningen på en sådan måde, at der kan være grundlag for strafansvar, udgøre en oplysning om et muligt strafbart forhold og dermed omfattet af persondatalovens § 8.

Oplysninger om straffe- og børneattester anses endvidere for omfattet af oplysninger om strafbare forhold efter persondatalovens § 8, stk. 1.

3.10.2.3. Offentlige myndigheders behandling af oplysninger om strafbare forhold
Persondatalovens § 8, stk. 1-3, omhandler, hvornår offentlige myndigheder kan behandle og videregive oplysninger om bl.a. strafbare forhold.

Det fremgår således af persondatalovens § 8, *stk. 1*, at der for den offentlige forvaltning ikke må behandles oplysninger om bl.a. strafbare forhold, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver. Det er således en forudsætning for den offentlige forvaltnings lovlige behandling af oplysninger om strafbare forhold, at et nødvendighedskriterium er opfyldt.

Et sådan nødvendighedskriterium vil eksempelvis være opfyldt i forbindelse med udbudsreglerne, hvorefter en ordregivende myndighed er pålagt at udelukke en ansøger eller en tilbudsgiver, når en person, som er medlem af ansøgerens eller tilbudsgiverens bestyrelse, direktion eller tilsynsråd, ved endelig dom er dømt eller har vedtaget et bødeforelæg for et kriminelt forhold, herunder eksempelvis bestikkelse af tjenestemænd, hvidvaskning eller straffelovens bestemmelser om børnearbejde og menneskehandel.

Det kunne også være en situation, hvor tilsynsmyndighederne på sundhedsområdet modtager oplysninger om, at en autoriseret sundhedsperson, eller en person der søger om at blive autoriseret, har begået en overtrædelse af straffeloven, der kan rejse tvivl om den pågældendes egnethed som eksempelvis læge.

For så vidt angår politi og anklagemyndigheden giver det ikke umiddelbart anledning til tvivl om, hvornår det er nødvendigt at behandle oplysninger om strafbare forhold.

Det samme gør sig gældende for andre myndigheder end politi og anklagemyndigheden, som efter lovgivningen fører tilsyn med bestemte retsområder, hvor overtrædelse af reglerne er strafsanktioneret, og hvis behandlingen af oplysninger om strafbare forhold er nødvendig for udførelsen af tilsynet og de dermed forbundne opgaver. Dette kan f.eks. være ved indgivelse af en politianmeldelse mv. Dette er en videreførelse af Registertilsynets praksis efter de tidligere regler i lov om offentlige myndigheders registre, som videreføres af Datatilsynet.[279]

I persondatalovens § 8, *stk. 2*, er spørgsmålet om den offentlige forvaltnings videregivelse af bl.a. oplysninger om strafbare forhold reguleret.

Registerudvalget anførte i betænkning nr. 1345[280], at der godt kunne udarbejdes regler om behandling af strafbare forhold, hvor der kunne stilles større krav til eksempelvis videregivelse af oplysninger om strafbare forhold end til indsamling og registrering af sådanne oplysninger.

Det fremgår således af persondatalovens § 8, *stk. 2*, at offentlige myndigheder ikke må videregive oplysninger om bl.a. strafbare forhold. Det fremgår endvidere, at der alene kan ske videregivelse af oplysninger om strafbare forhold, såfremt én af betingelserne i lovens § 8, stk. 2, *nr. 1-4*, er opfyldt. Det skal desuden bemærkes, at spørgsmålet om videregivelse fra forvaltningsmyndigheder, der udfører opgaver inden for det sociale område, er reguleret i bestemmelsens *stk. 3*.

Det fremgår af bemærkningerne til persondataloven, at § 8, *stk. 2*, både omfatter spørgsmålet om videregivelse fra en offentlig myndighed til private og til andre offentlige myndigheder.[281]

Det fremgår af lovens § 8, stk. 2, *nr. 1*, at der kan ske videregivelse af oplysninger om bl.a. strafbare forhold, hvis den registrerede har givet samtykke til videregivelsen. Hertil kræves, at kravene til samtykke efter persondatalovens § 3, nr. 8, er opfyldt. Dernæst kan der ske videregivelse efter bestemmelsens *nr. 2*, hvis videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelsen, herunder hensynet til den, oplysningen angår.

[279] Persondataloven med kommentarer (2015), s. 310-311.
[280] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 243-244.
[281] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 8.

Disse hensyn kan bl.a. – efter en konkret vurdering – være væsentlige hensyn til forbrugerbeskyttelse, folkesundheden eller miljøbeskyttelse, jf. betænkning 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater mv.[282]

Der kan f.eks. være tale om, at en tilsynsmyndighed på sundhedsområdet – efter en konkret vurdering – videregiver oplysninger om strafbare forhold begået af en autoriseret sundhedsperson til den region, hvor en autoriseret sundhedsperson er ansat, eller til en tilsynsmyndighed i et andet land, hvor den pågældende har ret til at udøve hverv som sundhedsperson.

Herudover følger det af bestemmelsens *nr. 3*, at der kan ske videregivelse, når videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller er påkrævet for en afgørelse, som myndigheden skal træffe. Til sidst kan en offentlig myndighed på baggrund af § 8, stk. 2, *nr. 4*, videregive oplysninger om bl.a. strafbare forhold, når det er nødvendigt for udførelsen af en persons eller virksomheds opgaver for det offentlige.

Spørgsmålet om videregivelse fra forvaltningsmyndigheder inden for det sociale område er reguleret ved persondatalovens § 8, *stk. 3*. Det fremgår af bestemmelsen, at forvaltningsmyndigheder, der udfører opgaver inden for det sociale område, må videregive oplysninger om bl.a. strafbare forhold, hvis betingelserne i § 8, stk. 2, *nr. 1* eller *nr. 2*, er opfyldt, eller hvis videregivelsen er et nødvendigt led i sagens behandling eller nødvendig for, at en myndighed kan gennemføre tilsyns – eller kontrolopgaver.

Det fremgår af bemærkningerne til loven, at kriterierne for videregivelse svarer til dem, der er fastsat i forvaltningslovens § 28, stk. 2.[283] Det bemærkes, at forvaltningslovens § 28 siden da er blevet ændret. Persondatalovens § 8, *stk. 3,* regulerer også videregivelse fra forvaltningsmyndigheder inden for det sociale område til private såvel som offentlige dataansvarlige.

Det fremgår endvidere af bemærkningerne til persondataloven[284], at bestemmelsen omfatter myndigheder, der varetager opgaver inden for det sociale område. Ifølge bemærkningerne drejer dette sig navnlig om bl.a. kommunernes og regionernes socialforvaltninger samt de statslige myndigheder, der varetager opgaver på det sociale område.

[282] Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave, (2013), s. 804-805.
[283] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 8.
[284] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 8.

Som rettesnor kan det lægges til grund, at myndigheder, som er omfattet af den sociale retssikkerhedslov, falder inden for anvendelsesområdet af persondatalovens § 8, *stk. 3*.

For så vidt angår myndigheder, som varetager opgaver både inden og uden for det sociale område, må det antages, at § 8, *stk. 3*, kun finder anvendelse i de tilfælde, hvor myndigheden udfører opgaver inden for det sociale område.[285] Det betyder, at hvor en myndighed både udfører opgaver inden for og uden for det sociale område, kan bestemmelsen kun antages at finde anvendelse i de tilfælde, hvor myndigheden konkret udfører opgaver inden for det sociale område.[286]

Herudover kan § 8, *stk. 3*, fraviges ved anden lovgivning.[287] I sådanne tilfælde er der fastsat særlige bestemmelser om adgang til at videregive og udveksle oplysninger, hvorved persondatalovens § 8, stk. 3, ikke finder anvendelse.

Persondatalovens § 8, stk. 3, er i en række tilfælde fraveget i dansk ret, eksempelvis i lov om Udbetaling Danmark.

Endvidere fremgår det af persondatalovens § 8, *stk. 6*, at behandling af oplysninger i de tilfælde, der er reguleret i § 8, stk. 1, 2, 4 og 5, i øvrigt kan finde sted, hvis betingelserne i § 7 er opfyldt. Der henvises i den forbindelse til afsnit 3.7. om følsomme oplysninger, artikel 9, stk. 1.

Endelig fremgår det af persondatalovens § 8, *stk. 7*, at et fuldstændigt register over straffedomme kun må føres for en offentlig myndighed.

3.10.2.4. Privates behandling af oplysninger om strafbare forhold

Som anført ovenfor fremgår det af direktivets artikel 8, stk. 5, 1. pkt., at andre end offentlige myndigheder kun kan behandle oplysninger om bl.a. strafbare forhold, hvis der i medlemsstaternes nationale ret gives tilstrækkelige, specifikke garantier.

Registerudvalget anførte i betænkning nr. 1345, at der på denne baggrund burde fastsættes særlige regler om, hvornår behandling af oplysninger om strafbare forhold kunne finde sted i dansk lovgivningen, herunder privates behandling af oplysninger om strafbare forhold.[288]

[285] Persondataloven med kommentarer (2015), s. 314ff.
[286] Persondataloven med kommentarer (2015), s. 315.
[287] Persondataloven med kommentarer (2015), s. 316.
[288] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 241.

For så vidt angår fastsættelsen af tilstrækkelige, specifikke garantier i medfør af national lov, anførte Registerudvalget endvidere i betænkningen[289], at det stemte bedst overens med kravene efter direktivets artikel 8, stk. 5, at der i dansk ret blev fastsat snævre betingelser for private dataansvarliges behandling af oplysninger om strafbare forhold.

På denne baggrund er der i persondatalovens § 8, *stk. 4* og *5*, skabt mulighed for, at private dataansvarlige – efter snævre betingelser – bl.a. kan behandle og videregive oplysninger om strafbare forhold, herunder oplysninger om straffe- og børneattester.

Det fremgår af lovens § 8, *stk. 4*, at private kan behandle oplysninger om bl.a. strafbare forhold, hvis den registrerede har givet udtrykkeligt samtykke hertil.

Det fremgår endvidere af lovens § 8, stk. 4, *2. pkt.*, at private kun kan behandle oplysninger om bl.a. strafbare forhold uden samtykke fra den registrerede, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede.

Det fremgår af bemærkningerne til persondataloven, at formålet med § 8, *stk. 4, 2. pkt.*, er at opstille meget snævre rammer for, hvornår der kan ske registrering af følsomme oplysninger uden samtykke.[290]

Det fremgår endvidere af bemærkningerne[291], at lovens § 8, stk. 4, 2. pkt., giver mulighed for, at en virksomhed kan registrere oplysninger om strafbare forhold med henblik på indgivelse af politianmeldelse, f.eks. om butikstyveri og eventuel senere afgivelse af vidneforklaring i retten. Hertil bemærkes det dog, at oplysningerne dog skal destrueres snarest muligt, jf. persondatalovens § 5, stk. 5.

Det følger af Registertilsynets praksis, at private efter § 8, stk. 4, formentlig har mulighed for at registrere oplysninger om strafbare forhold med henblik på indgivelse af politianmeldelse, f.eks. hvis der er formodning om tyveri begået mod den private.[292]

Endvidere muliggør bestemmelsen – ifølge bemærkningerne hertil – at humanitære organisationer mv., såsom Amnesty International, uden den pågældendes samtykke kan behandle

[289] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 245.
[290] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 8.
[291] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 8.
[292] Registertilsynets Årsberetning 1997, s. 85-87, gengivet i Persondataloven med kommentarer (2015), s. 318.

oplysninger om strafbare forhold, f.eks. fordi den registrerede ikke kan findes, eller fordi det ikke har været muligt at rette henvendelse til den pågældende som følge af fængsling eller lignende.

Herudover er privates mulighed for at behandle oplysninger i et fuldstændigt register over straffedomme afskåret efter persondatalovens § 8, *stk. 7*.

3.10.2.5. Særligt om behandling af oplysninger om straffe- og børneattester
Oplysninger om borgeres lovovertrædelser til brug for bl.a. udarbejdelse og udlevering af børne- og straffeattester er i det Centrale Kriminalregister. Reguleringen af videregivelse af oplysninger, bl.a. straffedomme, følger af persondatalovens § 8, men også af kriminalregisterbekendtgørelsen[293], som er udstedt i medfør af persondatalovens § 32, stk. 5, og § 72. Efter kriminalregisterbekendtgørelsen kan der i nærmere bestemt omfang videregives oplysninger fra Det Centrale Kriminalregister til private virksomheder og offentlige myndigheder. Endvidere har registrerede personer i et nærmere bestemt omfang adgang til indsigt i oplysninger om sig selv. Der kan efter disse regler udleveres forskellige typer af attester i forbindelse med f.eks. stillingsansøgninger.

Endvidere indeholder børneattestloven nærmere regler om indhentelse af børneattester.[294]

Datatilsynet[295] har i en udtalelse til Folketingets Ombudsmand om en kommunes indhentelse af straffeattester bemærket, at såfremt en kommune indscanner en privat straffeattest, således at attestens fulde indhold findes elektronisk i kommunens sagsbehandlings- og dokumenthåndteringssystem, vil der være tale om elektronisk databehandling af personoplysninger, jf. persondatalovens § 1.

Det skal endvidere bemærkes, at det fremgår af bemærkningerne til persondataloven[296], at spørgsmålet om indhentelse af oplysninger i ansøgningssager ved offentlige myndigheder eller om pligt til videregivelse af oplysninger ikke reguleres af persondataloven. I stedet gælder reglerne i forvaltningslovens § 29 og § 31 også i relation til denne behandling af personoplysninger.

[293] Bekendtgørelse nr. 881 af 4. juli 2014 med senere ændringer om behandling af personoplysninger i det Centrale Kriminalregister.
[294] Lovbekendtgørelse nr. 362 af 2. april 2014 om bekendtgørelse af lov om indhentelse af børneattest i forbindelse med ansættelse af personale mv.
[295] Datatilsynets j.nr. 2010-321-0308 af 15. oktober 2010.
[296] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.11.3. i de almindelige bemærkninger.

For så vidt angår behandling af oplysninger om straffe- og børneattester på baggrund af persondatalovens regler, skal betingelserne for behandling af oplysninger om strafbare forhold i lovens § 8 iagttages.

For offentlige myndigheder betyder det, at der kan ske behandling af oplysninger om straffe- og børneattester på baggrund af den registreredes samtykke i medfør af persondatalovens § 8, stk. 1, jf. § 8, stk. 6, jf. § 7, stk. 2, nr. 1, medmindre der er tale om en ansøgningssag i det offentlige.

Det samme gør sig gældende for private, der kan behandle oplysninger om straffe- og børneattester på baggrund af den registreredes samtykke i medfør af persondatalovens § 8, stk. 4.

I praksis må det antages, at den registrerede oftest vil give samtykke til indhentelse af en straffeattest i en mulig ansættelsessituation.[297] I sådanne tilfælde vil betingelserne for behandling af oplysninger om straffe- og børneattester være opfyldt, jf. persondatalovens § 8, stk. 1, jf. § 8, stk. 6, jf. § 7, stk. 2, nr. 1, og § 8, stk. 4.

Hvis en ansøger til et job selv rekvirerer sin private straffeattest fra politiet og frivilligt indsender denne til ansøgerstedet, må dette anses for at udgøre et gyldigt samtykke til behandlingen.[298]

Opbevaring af straffeattester på personalesager for offentlige myndigheder kan ske med hjemmel i persondatalovens § 8, stk. 1. Dette gælder i det tilfælde, hvor indhentelsen af en straffeattest sker på baggrund af et samtykke efter forvaltningslovens § 29 og med hjemmel i § 22 og § 36 i kriminalregisterbekendtgørelsen (henholdsvis den offentlige straffeattest og børneattesten). Hvis der er tale om en privat straffeattest, hvor indhentelse sker på grundlag af et samtykke, kan offentlige myndigheder endvidere opbevare disse i medfør af persondatalovens § 8, stk. 1, såfremt det i forhold til den konkrete stilling vurderes at være sagligt og proportionalt at indhente en privat straffeattest, således at betingelserne i persondatalovens § 5, stk. 2 og 3, er opfyldt.

Udover behandlingsbetingelsen i lovens § 8, skal de grundlæggende principper i lovens § 5 – ligesom ved al anden behandling af personoplysninger – iagttages, når der behandles oplysninger om straffe- og børneattester. Det fremgår af persondatalovens § 5, *stk. 1*, at behandlingen skal ske i overensstemmelse med god databehandlingsskik. Herudover skal indsamlingen af straffe- og børneattester efter lovens § 5, *stk. 2*, ske til udtrykkeligt angiv-

[297] Michael Gøtze, Juristen nr. 5/2010, s. 147.
[298] Michael Gøtze, Juristen nr. 5/2010, s. 147.

ne og ikke mindst saglige formål, og senere behandling ikke må være uforenelig med disse formål.

Det skal således stå klart, til hvilke formål straffe- og børneattesten skal bruges til, og dette formål skal være sagligt. Det må f.eks. antages ikke at være i overensstemmelse med persondatalovens § 5, hvis der indsamles oplysninger om en straffe- eller børneattester, når der ikke aktuelt er noget at bruge denne til, men blot en forventning om, at der senere viser sig et formål.[299]

Dernæst skal behandling af oplysninger om straffe- og børneattester efter lovens § 5, *stk. 3*, være relevant og tilstrækkelig og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles. Den dataansvarlige er således efter § 5, *stk. 3*, undergivet et proportionalitetsprincip.

I forhold til behandlingen af oplysninger om straffe- og børneattest sætter persondatalovens § 5, *stk. 1-3*, dermed krav om saglighed og proportionalitet og sætter grænser for, i hvilke tilfælde der kan behandles oplysninger om strafbare forhold ved en straffe- og børneattest.

Det beror på en konkret vurdering i den enkelte behandlingssituation, om behandling af en straffe- eller børneattest kan anses for saglig og proportional og dermed i overensstemmelse med persondatalovens § 5.

Datatilsynet[300] har i den ovennævnte udtalelse om indhentelse af straffeattester til Folketingets Ombudsmand bemærket, at en generel politik i en kommune om, at der i forhold til alle stillinger standardmæssigt skal indhentes straffeattester på ansøgere, som kommunen påtænker at ansætte, efter tilsynets vurdering ikke var i overensstemmelse med persondatalovens § 5.

Datatilsynet fandt endvidere i udtalelsen, at det må bero på en konkret vurdering i de enkelte ansættelsessituationer, om indhentelse af en privat straffeattest kan anses for saglig og proportional og dermed i overensstemmelse med persondatalovens § 5.

3.10.3. Databeskyttelsesforordningen

Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger er reguleret i forordningens artikel 10.

[299] Se bl.a. Datatilsynets udtalelse, j. nr. 2010-321-0308.
[300] Datatilsynets j.nr. 2010-321-0308 af 15. oktober 2010.

Det fremgår af artikel 10, 1. pkt., at behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på grundlag af artikel 6, stk. 1, kun må foretages under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for de registreredes rettigheder og frihedsrettigheder. For så vidt angår bestemmelsens 2. pkt., henvises til afsnit 3.11. om register over straffedomme, artikel 10, 2. pkt.

Ligesom i databeskyttelsesdirektivet er der ikke i forordningen taget stilling til, hvad der skal forstås ved udtrykket *personoplysninger vedrørende straffedomme, lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger*.

For så vidt angår forholdet mellem forordningens artikel 10, 1. pkt., og databeskyttelsesdirektivets artikel 8, stk. 5, 1. afsnit, ses indholdet af de to udtryk på baggrund af en ordlydsfortolkning at være ens.

På denne baggrund – og idet det forudsættes, at udtrykket "strafbare forhold" fortolkes i lyset af forordningens artikel 10, 1. pkt. – må det antages, at betegnelsen i forordningen er en videreførelse af gældende ret for så vidt angår betegnelsen "strafbare forhold".

3.10.3.1. Offentlige myndigheders behandling af oplysninger om strafbare forhold
Det fremgår som nævnt af forordningens artikel 10, 1. pkt., første led, at oplysninger om strafbare forhold på grundlag af artikel 6, stk. 1, kun må foretages under kontrol af en offentlig myndighed.

I modsætning til databeskyttelsesdirektivets artikel 8, stk. 5, angives det materielle behandlingsgrundlag for offentlige myndigheders behandling af oplysninger om strafbare forhold direkte i artikel 10, 1. pkt. Der henvises således til forordningens artikel 6, stk. 1, som behandlingsgrundlag for offentlige myndigheders behandling og videregivelse af oplysninger om strafbare forhold. Artikel 6, stk. 1, omhandler lovlig behandling af ikke-følsomme oplysninger. Det betyder, at oplysninger om strafbare forhold skal anses for almindelige personoplysninger, og således ikke er omfattet af de særlige behandlingsregler for følsomme oplysninger i forordningens artikel 9.

Det fremgår dog af forordningens artikel 6, stk. 2 og 3, at medlemsstaterne har mulighed for, inden for rammerne af artikel 6, stk. 1, litra c og e, at opretholde og indføre mere specifikke bestemmelser for behandling af ikke-følsomme oplysninger for at tilpasse anvendelsen af databeskyttelsesforordningen. Det skal hertil bemærkes, at medlemsstaternes mulighed for – på baggrund af forordningen – at fastsatte nationale regler overordnet ikke vil være en ændring i forhold til gældende ret. Der henvises i øvrigt til afsnit 3.3. om be-

handling af ikke-følsomme oplysninger, artikel 6, stk. 1, og afsnit 3.4. om lovlig behandling af ikke-følsomme oplysninger – nationalt råderum, artikel 6, stk. 2 og 3.

Det må antages, at det umiddelbart er muligt at videreføre de særlige regler i gældende ret for henholdsvis behandling og videregivelse af oplysninger om strafbare forhold for offentlige myndigheder i medfør af persondatalovens § 8, *stk. 1-3*, på baggrund af forordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2 og 3.

Bestemmelsen i persondatalovens § 8, stk. 1-3, må endvidere, for så vidt angår "strafbare forhold", antages at leve op til kravet om at udgøre specifikke bestemmelser om anvendelse af forordningen, ved at der fastsættes mere præcise, specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling i overensstemmelse med forordningens artikel 6, stk. 2.

Persondatalovens § 8, *stk. 1*, omhandler, hvornår en afgrænset kreds af dataansvarlige må behandle en bestemt type af personoplysninger. Endvidere omhandler bestemmelsen *ikke* offentlige myndigheders *videregivelse* af personoplysninger, hvorfor der også stilles specifikke betingelser for, hvilken type af behandling der må foretages af offentlige myndigheder.

Herudover fastsættes der et generelt forbud mod, at offentlige myndigheder videregiver oplysninger om strafbare forhold efter persondatalovens § 8, *stk. 2*. Offentlige myndigheder kan herefter alene videregive sådanne oplysninger, hvis betingelserne i bestemmelsens nr. 1-4, er opfyldt.

I lighed med § 8, stk. 1, fastsættes der således i § 8, *stk. 2*, regler for, hvornår en bestemt kreds af dataansvarlige må foretage en specifik form for behandling af en bestemt type af personoplysninger.

Endelig fastsættes det i persondatalovens § 8, *stk. 3*, hvornår forvaltningsmyndigheder, der udfører opgaver inden for det sociale område, må videregive oplysninger om strafbare forhold. På samme måde som efter *stk. 2* og *3*, omhandler bestemmelsen, hvornår en bestemt kreds af dataansvarlige inden for den offentlige forvaltning må foretage en specifik form for behandling af en bestemt type af personoplysninger.

3.10.3.2. Privates behandling af oplysninger om strafbare forhold

Som nævnt fremgår det af forordningens artikel 10, 1. pkt., første led, at behandling af oplysninger om strafbare forhold som udgangspunkt kun må foretages under kontrol af en offentlig myndighed.

Private kan efter forordningens artikel 10, 1. pkt., sidste led, alene behandle oplysninger om strafbare forhold, hvis behandlingen har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder.

Det fremgår af persondatalovens § 8, stk. 4 og 5, at behandlingsgrundlaget for privates behandling og videregivelse af oplysninger om strafbare forhold er henholdsvis samtykke og en værdispringsregel.

Det må antages, at persondatalovens § 8, stk. 4 og 5, for så vidt angår behandling af *strafbare forhold* som udgangspunkt kan videreføres i sin helhed inden for artikel 10, 1. pkt., sidste led.

Herefter skal den pågældende bestemmelse endvidere give passende garantier for registreredes rettigheder og frihedsrettigheder i medfør af forordningens artikel 10, 1. pkt.

For så vidt angår forholdet mellem forordningens artikel 10, 1. pkt., og databeskyttelsesdirektivets artikel 8, stk. 5, 1. afsnit, ses indholdet af de to bestemmelser på baggrund af en ordlydsfortolkning at være ens.

Der er dog få sproglige ændringer, som det kan være relevant at vurdere. I databeskyttelsesdirektivet tales der om, *hvis der gælder tilstrækkelige, specifikke, garantier i medfør af den nationale lovgivning*, hvor der i forordningen tales om, at *hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder.*

De sproglige forskelle ses dog ikke at have en indholdsmæssig betydning i forhold til gældende ret, idet private fortsat kun kan behandle oplysninger om strafbare forhold, hvis det er i medfør af medlemsstatens nationale lovgivning, hvor der gives passende garantier for den registreredes rettigheder og frihedsrettigheder.

Der er som nævnt i persondatalovens § 8, *stk. 4* og *5*, fastsat snævre betinger for, hvornår private kan behandle oplysninger om bl.a. oplysninger om strafbare forhold, som antages at udgøre *specifikke, tilstrækkelige garantier* i overensstemmelse med kravene efter direktivets artikel 8, stk. 5.[301]

[301] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 245.

Det må derfor antages, at en videreførelse af retsstillingen i disse snævre betingelser i en national særregel ligeledes må anses for at udgøre *passende garantier* for den registreredes rettigheder og frihedsrettigheder i overensstemmelse med artikel 10, 1. pkt.

3.10.3.3. Særligt om behandling af oplysninger om straffe- og børneattester
Kravene om saglighed, formål og proportionalitet i databeskyttelsesforordningens artikel 5 er overordnet set en videreførelse af gældende ret efter persondatalovens § 5. Der henvises i øvrigt til afsnit 3.1. om principper for behandling af personoplysninger, artikel 5 og artikel 6, stk. 4.

Det må på den baggrund antages, at kravene efter persondatalovens § 5, for så vidt angår offentlige myndigheder og privates behandling af straffe- og børneattester på baggrund af et samtykke fra den registrerede, vil kunne videreføres på baggrund databeskyttelsesforordningens artikel 5.

Udover reglerne i persondatalovens § 8, er spørgsmål om videregivelse af oplysninger om bl.a. straffedomme reguleret i kriminalregisterbekendtgørelsen, som er udstedt i medfør af persondatalovens § 32, stk. 5, og § 72.

Det må antages, at bemyndigelsesbestemmelsen i persondatalovens § 72, hvorved vedkommende minister i særlige tilfælde kan fastsætte nærmere regler for behandlinger, som udføres for den offentlige forvaltning, kan videreføres inden for rammerne af forordningens artikel 6, stk. 2-3, jf. artikel 6, stk. 1, litra e.

Det må endvidere antages, at kriminalregisterbekendtgørelsen kan opretholdes på baggrund af forordningens artikel 6, stk. 2-3, jf. artikel 6, stk. 1, litra e. Kriminalregisterbekendtgørelsen må desuden antages at leve op til kravet om at udgøre specifikke bestemmelser om anvendelse af forordningen ved, at der fastsættes mere præcise specifikke krav til behandling af personoplysninger i Det Centrale Kriminalregister i overensstemmelse med forordningens artikel 6, stk. 2.

3.10.4. Overvejelser
Det fremgår af databeskyttelsesforordningens artikel 10, 1. pkt., at oplysninger om strafbare forhold på grundlag af artikel 6, stk. 1, kun må foretages under kontrol af en offentlig myndighed.

Det må antages, at det umiddelbart er muligt at videreføre de særlige regler i gældende ret for offentlige myndigheders behandling og videregivelse af oplysninger om strafbare for-

hold efter persondatalovens § 8, stk. 1-3, på baggrund af forordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2 og 3.

For så vidt angår privates behandling af oplysninger om strafbare forhold, ses forordningens artikel 10, 1. pkt., at være en videreførelse af gældende ret, idet private fortsat kun kan behandle oplysninger om strafbare forhold, hvis dette er på baggrund af medlemsstatens nationale lovgivning, hvor der gives passende garantier for den registreredes rettigheder og frihedsrettigheder.

Det kan derfor antages, at de "snævre betingelser" for privates behandling af oplysninger om strafbare forhold efter gældende ret vil kunne videreføres inden for rammerne af forordningens artikel 10, 1. pkt., idet en sådan begrænsning må antages at udgøre *passende garantier* for den registreredes rettigheder og frihedsrettigheder.

3.11. Register over straffedomme, artikel 10, 2. pkt.

3.11.1. Præsentation

Efter persondatalovens § 8, stk. 7, er det alene offentlige myndigheder, der må føre et *fuldstændigt* register over straffedomme.

I databeskyttelsesforordningens artikel 10, 2. pkt., følger et krav om, at et *omfattende* register over straffedomme kun må føres under kontrol af en offentlig myndighed.

3.11.2. Gældende ret

Ved behandling af personoplysninger i forbindelse med behandling af oplysninger om strafbare forhold, herunder straffedomme, skal behandlingsbetingelserne i lovens § 8 samt de grundlæggende behandlingsprincipper i persondatalovens § 5 iagttages.

Persondatalovens § 8 regulerer, hvornår offentlige såvel som private dataansvarlige må behandle oplysninger om bl.a. strafbare forhold.

Det følger af persondatalovens § 8, stk. 7, at et *fuldstændigt* register over straffedomme kun må føres for en offentlig myndighed. Bestemmelsen, der har sin baggrund i direktivets artikel 8, stk. 5, indebærer, at private ikke må opbygge et fuldstændigt register over straffedomme.

Efter bestemmelsens ordlyd er det alene fuldstændige registre over straffedomme, som er omfattet af begrænsningen. Dette gælder både for så vidt angår manuelle og elektroniske

registre.[302] Et register anses for at være fuldstændigt i persondatalovens § 8, stk. 7's og artikel 8, stk. 5's forstand, når det indeholder oplysninger om samtlige afsagte straffedomme. Et eksempel på et fuldstændigt register over straffedomme er Det Centrale Kriminalregister.

Det betyder omvendt, at eksisterende private retsinformationssystemer, som ikke indeholder oplysninger om samtlige afsagte straffedomme, ikke er omfattet af persondatalovens § 8, stk. 7. Behandlingen af straffedomme i forbindelse med et ikke-fuldstændigt register skal herefter ske på baggrund af de øvrige behandlingsbetingelser i persondatalovens § 8 eller § 9.

Vurderingen af, om et register er *fuldstændigt* i bestemmelsens forstand relaterer sig således til, om samtlige straffedomme *på landsplan* er indeholdt i registret og ikke til, om en dataansvarlig fører et register over samtlige straffedomme, der relaterer sig til den pågældende dataansvarlige, f.eks. en arbejdsgivers register over ansattes straffedomme.

3.11.3. Databeskyttelsesforordningen

Det følger af databeskyttelsesforordningens artikel 10, 1. pkt., at behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på grundlag af artikel 6, stk. 1, kun må foretages under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder.

Det følger herudover af artikel 10, 2. pkt., at ethvert omfattende register over straffedomme kun må føres under kontrol af en offentlig myndighed.

Et register er i artikel 4, nr. 6, defineret som enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt eller decentralt eller fordelt på funktionsbestemt eller geografisk grundlag.

Ifølge artikel 10, 2. pkt., er det således *omfattende* registre over straffedomme, som ikke må føres af private. Dette udgør umiddelbart en sproglig ændring i forhold til den tilsvarende i bestemmelse i databeskyttelsesdirektivets artikel 8, stk. 5, der begrænser sig til *fuldstændige* registre over straffedomme.

I den engelske sprogudgave af databeskyttelsesdirektivets artikel 8, stk. 5, 2. pkt., følger det ligeledes, at:

[302] Persondataloven med kommentarer (2015), s. 321.

> "However, a *complete* register of criminal convictions may be kept only under the control of official authority"

Til sammenligning følger det af den engelske sprogudgave af forordningens artikel 10, 2. pkt., at:

> "Any *comprehensive* register of criminal convictions shall be kept only under the control of official authority."

I den engelske sprogudgave af henholdsvis direktivet og forordningen er der således den samme forskel som i den danske sprogversion i betegnelsen af de registre over straffedomme, der alene må føres under kontrol af en offentlig myndighed.

På den anden side kan der henvises til den svenske sprogudgave af artikel 8, stk. 5, i databeskyttelsesdirektivet, hvoraf det fremgår, at:

> "Ett *fullständigt* register över brottmälsdomar får dock föras endast under kontroll av en myndighet."

Samtidig følger det af den svenske sprogudgave af forordningens artikel 10, 2. pkt., at:

> "Ett *fullständigt* register över fällande domar i brottmål får endast föras under kontroll av en myndighet."

Af den franske sprogudgave af direktivet følger det af artikel 8, stk. 5, at bestemmelsen alene omfatter et "*exhaustif*" (på dansk: *udtømmende, komplet* eller *fuldstændigt*) register over straffedomme:

> "Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique."

Den franske sprogudgave af forordningens artikel 10, 2., pkt., henviser til et "*complet"* (på dansk: *komplet, fuldstændigt* eller *samlet*) register over straffedomme:

> "Tout registre *complet* des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique."

De svenske og franske sprogudgaver af forordningen må isoleret set således anses for at være udtryk for en videreførelse af direktivet for så vidt angår et *fuldstændigt* register over straffedomme, som alene må føres under kontrol af offentlige myndigheder.

Den sproglige fortolkning af den svenske såvel som den franske sprogudgave af bestemmelsen taler – i modsætning til den danske og engelske forståelse – således for, at der ikke

er tilsigtet en indholdsmæssig ændring af de registre over straffedomme, som er omfattet af direktivets artikel 8, stk. 5, og nu af forordningen artikel 10, 2. pkt.

Alle versioner af EU's officielle sprog er autentiske og de forskellige sproglige versioner af EU-retsakt skal fortolkes ensartet. En EU-bestemmelse, der er uoverensstemmende i forskellige sprogversioner, skal fortolkes på baggrund af den almindelige opbygning af og formålet med den ordning, som bestemmelsen indgår i, jf. EU-Domstolens dom i sag 30/77, Regina mod Bouchereau (præmis 14).

Det må antages, at vurderingen af, om et register kan anses for *omfattende/fuldstændigt*, heller ikke i forhold til forordningen skal basere sig på forholdene hos den dataansvarlige. Vurderingen må ligesom ved databeskyttelsesdirektivet i stedet antages at skulle ske ud fra en betragtning om, hvor *omfattende/fuldstændigt* det konkrete register er set i forhold til samtlige afsagte straffedomme i det pågældende EU-land.

Artikel 10, 2. pkt. er en konkret og fuldstændig begrænsning af private aktørers mulighed for at behandle oplysninger om straffedomme. Private aktørers mulighed for at behandle oplysninger om straffedomme beror i øvrigt på, at behandlingen er hjemlet i EU-retten (udover databeskyttelsesforordningen) eller i national lovgivning, jf. artikel 10, 1. pkt.

Spørgsmålet er, hvilken betydning de forskellige sproglige versioner af forordningens artikel 10, 2. pkt., har for den indholdsmæssige afgrænsning af, hvilke registre over straffedomme der efter forordningen ikke må føres af private.

Det pågældende register skal – udover at være omfattet af definitionen af et register – i hvert fald kunne betegnes som omfattende, før artikel 10, 2. pkt. finder anvendelse. Når der skal tages højde for sproglige versioner som den franske og svenske, skal det pågældende register nok også være grænsende til at være fuldstændigt for at blive omfattet af bestemmelsen.

Under alle omstændigheder må det betyde, at forholdet vil være omfattet af forordningens artikel 10, 2. pkt., hvis et register indeholder alle danske straffedomme med undtagelsen af straffedommene fra et lille afgrænset retsområde, da der i et sådant tilfælde vil være tale om et omfattende register, grænsende til et fuldstændigt register.

Det må dog antages, at den beskrevne uklarhed i de forskellige sprogversioner af forordningens artikel 10, 2. pkt., ikke kan eller vil få den store praktiske betydning.

3.11.4. Overvejelser

Med artikel 10, 2. pkt., er der i den danske sprogversion af forordningen tale om en sproglig ændring i forhold til gældende ret, idet det nu er *omfattende* frem for *fuldstændige* registre over straffedomme, som kun må føres under kontrol af en offentlig myndighed.

Det må imidlertid antages, at denne ændring ikke har væsentlig betydning for den indholdsmæssige eller praktiske afgrænsning af, hvilke registre over straffedomme, der efter forordningen ikke må føres af private. Et register over straffedomme vil alene skulle anses for *omfattende* efter forordningens artikel 10, 2. pkt., såfremt det er omfattende i forhold til samtlige afsagte straffedomme i Danmark.

3.12. Behandling, der ikke kræver identifikation, artikel 11

3.12.1. Præsentation

I artikel 11 i databeskyttelsesforordningen er der regler om behandling af personoplysninger, hvor formålet ikke kræver – eller ikke længere kræver – at den registrerede kan identificeres af den dataansvarlige. Reglerne indebærer, at den dataansvarlige ikke kan forpligtes til at behandle yderligere oplysninger blot for at overholde forordningen.

3.12.2. Gældende ret

Der er ikke i gældende ret en specifik bestemmelse om, hvordan en dataansvarlig skal forholde sig i det tilfælde, hvor der behandles personoplysninger, hvis formål ikke kræver eller ikke længere kræver, at den registrerede kan identificeres af den dataansvarlige.

Efter persondataloven og databeskyttelsesdirektivet må et tilfælde, hvor formålet med en behandling af personoplysninger ikke kræver eller ikke længere kræver, at den registrerede kan identificeres, efter dataminimeringsreglerne i lovens § 5, stk. 3, og direktivets artikel 6, stk. 1, litra c, umiddelbart føre til, at den dataansvarlige ikke (længere) må opbevare oplysninger, som gør det muligt for den dataansvarlige at identificere den registrerede.

Ultimativt kan det føre til, at oplysningerne ikke længere kan betragtes som personoplysninger, jf. persondatalovens § 3, nr. 1, og direktivets artikel 2, litra a, og at behandlingen derfor ikke længere er omfattet af persondatalovens og direktivets anvendelsesområde, jf. lovens § 1 og direktivets artikel 4.

Efter gældende ret er der dog også mulighed for, at behandling af oplysninger kan være omfattet af persondatalovens anvendelsesområde, selvom den dataansvarlige ikke umiddelbart kan identificere den registrerede.

Det er navnlig tilfældet, hvor den dataansvarlige behandler oplysninger om identificerbare – og ikke identificerede – fysiske personer.

Det bemærkes i den forbindelse, at der for at afgøre, om en person er identificerbar, skal tages alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den dataansvarlige eller af enhver anden person, jf. databeskyttelsesdirektivets præambelbetragtning nr. 26.

Det er således uden betydning for, om en fysisk person er identificerbar, om identifikationsoplysningen er alment kendt eller umiddelbart tilgængelig, hvorfor en oplysning også er identificerbar, hvor det kun for den indviede vil være muligt at forstå, hvem en oplysning vedrører, så længe der med rimelige midler kan findes frem til, hvem den pågældende er. Efter gældende ret skal der ikke meget til at statuere, at en oplysning vedrører en identificerbar fysisk person.[303]

En oplysning kan således godt vedrøre en *identificerbar* fysisk person og dermed være omfattet af begrebet "personoplysning" og persondataloven, uden at den dataansvarlige umiddelbart selv kan *identificere* den pågældende.

Efter persondataloven vil en dataansvarlig som udgangspunkt skulle iagttage oplysningspligten (lovens kapitel 8) og indsigtsretten (lovens kapitel 9) samt den registreredes øvrige rettigheder (lovens kapitel 10), når der behandles personoplysninger omfattet af persondatalovens anvendelsesområde, uanset om der behandles oplysninger om en identificerbar fysisk person, som den dataansvarlige ikke umiddelbart selv kan identificere.

I det tilfælde, hvor den dataansvarlige eksempelvis fra andre end den registrerede indhenter oplysninger om en identificerbar fysisk person, som den dataansvarlige ikke umiddelbart selv kan identificere, er den dataansvarlige efter persondatalovens § 29, stk. 1, således som udgangspunkt forpligtet til at indhente ydereligere oplysninger om den registrerede med henblik på at kunne identificere den pågældende og opfylde oplysningspligten. Dette gælder dog ikke, hvis det viser sig at være uforholdsmæssigt vanskeligt, jf. § 29, stk. 3, hvilket ofte er tilfældet for såkaldte bipersoner.

3.12.3. Databeskyttelsesforordningen

Det følger af forordningens artikel 11, stk. 1, at hvis formålene med en dataansvarligs behandling af personoplysninger ikke kræver eller ikke længere kræver, at den registrerede kan identificeres af den dataansvarlige, er den dataansvarlige ikke *forpligtet* til at beholde,

[303] Persondataloven med kommentarer (2015), s. 135-141.

indhente eller behandle yderligere oplysninger for at kunne identificere den registrerede alene med det formål at overholde denne forordning.

Af artikel 11, stk. 2, følger det, at hvis den dataansvarlige i tilfælde, der er omhandlet i artikel 11, stk. 1, kan påvise, at vedkommende ikke kan identificere den registrerede, underretter den dataansvarlige den registrerede herom, hvis det er muligt. I sådanne tilfælde finder den registreredes rettigheder opregnet i artikel 15-20 ikke anvendelse, medmindre den registrerede for at udøve sine rettigheder i henhold til disse artikler, giver yderligere oplysninger, der gør det muligt at identificere den pågældende.

Artikel 11 suppleres af præambelbetragtning nr. 57, hvorefter den dataansvarlige ikke bør være forpligtet til at indhente yderligere oplysninger for at identificere den registrerede udelukkende med det formål at overholde bestemmelserne i denne forordning, hvis de personoplysninger, der behandles af den dataansvarlige, ikke sætter vedkommende i stand til at identificere en fysisk person.

Bestemmelsen i *stk. 1* må i et vist omfang anses for at være en undtagelse til andre regler i forordningen i den situation, hvor formålet med behandlingen ikke kræver eller ikke længere kræver, at den registrerede kan identificeres af den dataansvarlige.

Udtrykket "den registrerede" i bestemmelsens stk. 1 må svare til definitionen af en identificerbar fysisk person i forordningens artikel 2, stk. 1, og artikel 4, nr. 1, (dog med den modifikation, at det i artikel 11 alene er relevant om den dataansvarlige – og ikke evt. tredjemand – kan identificere den registrerede).

Hvis formålet med en behandling ikke kræver eller ikke længere kræver, at den registrerede kan identificeres, må ordlyden af stk. 1 forstås således, at det ikke er *påkrævet* for den dataansvarlige at beholde, indhente eller i øvrigt at behandle oplysninger alene med henblik på at overholde andre bestemmelser i forordningen.

Dette kan ses i sammenhæng med forordningens dataminimeringsregel i artikel 5, stk. 1, litra c, hvorefter personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

Omvendt kan ordlyden af artikel 11, stk. 1, ("ikke forpligtet til") ikke antages på forhånd at udelukke en dataansvarlig fra at behandle personoplysninger (om identificerbare fysiske personer) med det formål at overholde forordningens øvrige regler, f.eks. oplysningspligten.

Dataansvarlige kan efter ordlyden af artikel 11, stk. 1, påberåbe sig bestemmelsen både i behandlingssituationer, hvor behandlingens formål *ikke kræver*, at den registrerede kan identificeres af den dataansvarlige, og situationer, hvor behandlingens formål ikke *længere* kræver identifikation.

Bestemmelsen fører til, at den dataansvarlige, som alene indhenter og behandler oplysninger om en identificerbar fysisk person, som den dataansvarlige ikke umiddelbart kan identificere, ikke er forpligtet til at indhente yderligere oplysninger for at identificere den registrerede udelukkende for at overholde bestemmelserne i forordningen, herunder oplysningspligten (artikel 13-14) og indsigtsretten (artikel 15).

For så vidt angår situationer, hvor behandlingens formål *ikke længere kræver*, at den registrerede kan identificeres af den dataansvarlige – underforstået at behandlingens formål tidligere *har* krævet identifikation – må artikel 11, stk. 1, efter sin ordlyd først kunne påberåbes af en dataansvarlig fra det tidspunkt, hvor formålene med vedkommendes behandling af personoplysninger ikke længere kræver identifikation af den registrerede.

Det bemærkes i den forbindelse, at artikel 11, stk. 1, ikke ændrer på de tidsmæssige krav for opfyldelse af oplysningspligten, der fremgår af forordningens artikel 13, stk. 2 (personoplysninger indsamlet hos den registrerede), og artikel 14, stk. 3-4 (personoplysninger ikke indsamlet hos den registrerede).

Det følger som nævnt af artikel 11, *stk. 2*, 1. pkt., at den dataansvarlige underretter den registrerede – hvis det er muligt – i situationer, hvor den dataansvarlige i tilfælde omhandlet i artikel 11, stk. 1, kan påvise, at vedkommende ikke kan identificere den registrerede. En sådan påvisning ville eksempelvis kunne være ved opslag i en myndigheds sagssystem eller lignende.

Hvis den dataansvarlige vil påberåbe sig artikel 11, stk. 1, og samtidig er i stand til at påvise, at han ikke (længere) kan identificere den registrerede, *skal* – jf. ordet "underretter" – den dataansvarlige således underrette den registrerede om påberåbelsen af artikel 11, jf. artikel 11, stk. 2, 1. pkt. Det kan f.eks. tænkes at være i en situation, hvor den dataansvarlige alene behandler den registreredes e-mailadresse uden at kunne identificere den registrerede ud fra e-mailadressen.

Denne underretningspligt gælder dog ikke, hvis underretning af den ikke-identificerede – men identificerbare – registrerede ikke er mulig, jf. artikel 11, stk. 2, 1. pkt., sidste led. Det kan ikke kræves, at den dataansvarlige indhenter yderligere oplysninger for at overholde underretningspligten, jf. princippet i artikel 11, stk. 1.

I de tilfælde, hvor den dataansvarlige påberåber sig artikel 11, stk. 1, og underretter den registrerede efter pligten hertil i artikel 11, stk. 2, 1. pkt., fordi underretning er mulig, finder artikel 15-20 om indsigtsret, berigtigelse, sletning, begrænset behandling, underretning og retten til dataportabilitet ikke anvendelse, jf. artikel 11, stk. 2, 2. pkt. I sådanne tilfælde, hvor underretning således *er* mulig, er der omvendt ikke gjort undtagelse fra f.eks. forordningens artikel 13-14 om dataansvarliges oplysningspligt.

Det fremgår dog også af artikel 11, stk. 2, 2. pkt., at artikel 15-20 alligevel gælder – på trods af underretning fra den dataansvarlige efter artikel 11, stk. 2 – hvis den registrerede for at udøve sine rettigheder i henhold til artikel netop 15-20, giver yderligere oplysninger, der gør det muligt at identificere den pågældende.

Det følger i forlængelse heraf af forordningens artikel 12, der indeholder generelle bestemmelser vedrørende forordningens kapitel III om de registreredes rettigheder, at i de tilfælde, der er omhandlet i artikel 11, stk. 2, må den dataansvarlige ikke afvise at efterkomme den registreredes anmodning om at udøve sine rettigheder i henhold til artikel 15-22, medmindre den dataansvarlige påviser, at vedkommende ikke er i stand til at identificere den registrerede, jf. artikel 12, stk. 2, 2. pkt.

3.12.4. Overvejelser

Forordningens artikel 11, stk. 1, er ny i forhold til databeskyttelsesdirektivet, idet den udtrykkeligt gør det muligt for dataansvarlige at gøre undtagelse fra forordningens regler, i det omfang overholdelsen ville kræve behandling af yderligere oplysninger, end der er behov for.

3.13. Retsinformation

3.13.1. Præsentation

Formålet med retsinformationssystemer er at stille afgørelser og domme til rådighed for en bredere kreds for at sikre en ensartet retsanvendelse. Dette vil medføre, at der skabes mere åbenhed og øget indsigt i afgørelser og domme, både for borgere og mere professionelle brugere såsom Folketinget, advokater, universiteter og medier mv.

Efter dansk ret kan følsomme oplysninger efter persondatalovens § 9, stk. 1, behandles med henblik på at føre retsinformationssystemer af væsentlig betydning, hvis behandlingen er nødvendig for førelsen af systemerne.

Det vil i det følgende blive vurderet, om der i databeskyttelsesforordningen er mulighed for at videreføre en hjemmel svarende til persondatalovens § 9 om retsinformationssystemer. For så vidt angår registre over straffedomme henvises til afsnit 3.11.

3.13.2. Gældende ret

3.13.2.1. Persondatalovens behandlingsregler

Ved behandling af personoplysninger i forbindelse med førelse af et retsinformationssystem skal de grundlæggende behandlingsprincipper i persondatalovens § 5 og behandlingsbetingelserne i lovens §§ 6 og 9 iagttages.

Ikke-følsomme personoplysninger kan bl.a. behandles, hvis det er nødvendigt af hensyn til udførelsen af en opgave i samfundets interesse, jf. lovens § 6, stk. 1, nr. 5.

Ifølge persondatalovens § 9, stk. 1, kan oplysninger omfattet af §§ 7 og 8 – som ellers ikke vil kunne behandles – behandles med henblik på at føre retsinformationssystemer af væsentlige samfundsmæssige betydning, hvis behandlingen er nødvendig for førelsen af systemerne. Efter § 9, stk. 2, må sådanne oplysninger ikke senere behandles i andet øjemed. Det samme gælder for behandlinger af ikke-følsomme oplysninger, som alene foretages med henblik på at føre retsinformationssystemer. Endvidere følger det af § 9, stk. 3, at tilsynsmyndigheden kan meddele nærmere vilkår for de i stk. 1 nævnte behandlinger. Tilsvarende gælder for de i § 6 nævnte oplysninger, som alene behandles i forbindelse med førelsen af retsinformationssystemer.

Af bemærkningerne til persondatalovens § 9[304] fremgår det bl.a., at nødvendighedskravet i stk. 1 betyder, at bestemmelsen ikke hjemler adgang til at behandle oplysninger i et retsinformationssystem, hvis systemet kunne tjene sit formål ligeså sikkert og effektivt uden oplysninger om enkeltpersoner. Det fremgår endvidere, at bestemmelsen i stk. 2 indebærer, at oplysningerne ikke må anvendes til at træffe foranstaltninger eller afgørelser vedrørende registrerede personer, og at dette gælder behandling af både følsomme oplysninger og ikke-følsomme oplysninger, som i henhold til §§ 6 og 9 alene foretages med henblik på at føre retsinformationssystemer. Desuden fremgår det, at oplysningerne naturligvis må anvendes i forbindelse med f.eks. førelse af en retssag, idet en sådan anvendelse ikke ligger uden for formålet med et retsinformationssystem. Om stk. 3 fremgår det, at bestemmelsen sikrer, at der kan fastsættes vilkår for behandling af følsomme oplysninger og nærmere vilkår for ikke-følsomme oplysninger, som alene sker i tilknytning til førelsen af retsinformationssystemer. Der kan f.eks. fastsættes vilkår om, at personnavne, præcise adresseangivelser og eventuelt andre identifikationsoplysninger fjernes i samme omfang, som det-

[304] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 9.

te skal ske efter Justitsministeriets cirkulære nr. 85 af 8. juli 1988 om indlæggelse af afgørelser i Retsinformation.

Det fremgår af Registerudvalgets betænkning[305], at retsinformationssystemer, som ikke var reguleret af registerlovene, skulle være reguleret af persondataloven, i det omfang de indeholdt personoplysninger, som konsekvens af databeskyttelsesdirektivet. Desuden fremgår det, at bestemmelsen i § 9, stk. 1, er indsat på baggrund af artikel 8, stk. 4, ifølge hvilken der af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, kan fastsættes undtagelser fra artikel 8, stk. 1, om forbud mod behandling af følsomme oplysninger (gennemført ved persondatalovens § 7, stk. 1), såfremt der gives tilstrækkelige garantier. Endelig fremgår det, at der med indsættelsen af bestemmelserne i persondatalovens § 9, stk. 3, hvorefter tilsynsmyndigheden kan fastsætte nærmere vilkår for behandlinger, der alene finder sted med henblik på at føre retsinformationssystemer, etableres tilstrækkelige garantier, og at der yderligere bidrages til etableringen heraf ved fastsættelsen af begrænsningen af behandling af oplysninger i § 9, stk. 2.

3.13.2.2. Datatilsynets praksis om retsinformationssystemer med videregivelse af domme
Det fremgår af Datatilsynets hjemmeside[306] og årsberetning fra 2001[307], at tilsynet har fastsat standardvilkår for retsinformationssystemer med videregivelse af afgørelser og domme.

Det fremgår af den nævnte årsberetning[308], at udgangspunktet efter Datatilsynets opfattelse er, at der ikke må videregives oplysninger om enkeltpersoners rent private forhold, dvs. følsomme oplysninger omfattet af lovens §§ 7 og 8, og at hovedlinjen med hensyn til ikke-følsomme oplysninger efter tilsynets opfattelse må være, om der er tale om fortrolige oplysninger, hvilket svarer til Datatilsynets vilkår vedrørende offentliggørelse af myndigheders afgørelser. Det fremgår endvidere, at Datatilsynet udtalte, at det må accepteres, at der offentliggøres ikke-fortrolige oplysninger uden nogen form for anonymisering, jf. persondataloven § 6, stk. 1, nr. 5 og 7. Derudover fremgår det, at der tilbage stod spørgsmålet om de "fortrolige" oplysninger, hvor der efter tilsynets opfattelse i visse tilfælde vil skulle ske anonymisering. Datatilsynet fandt anledning til at medtage et vilkår om, at der yderligere skal ske anonymisering, hvis forholdene særligt tilsiger dette, for at sikre, at der sker anonymisering af fortrolige oplysninger i de tilfælde, som ikke omfattes af de øvrige vilkår, og hvor videregivelse uden anonymisering ikke kan ske inden for rammerne af lovens § 6, stk. 1, og § 9, stk. 1.

[305] Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 190-191 og 251-252.
[306] Se Datatilsynets vejledning om retsinformationssystemer, der er tilgængelig på tilsynets hjemmeside.
[307] Datatilsynets årsberetning 2001, s. 43-45.
[308] Datatilsynets årsberetning 2001, s. 47-49.

På baggrund af sagen har Datatilsynet fastsat standardvilkår for retsinformationssystemer med videregivelse af afgørelser og domme.

Det fremgår af ovennævnte årsberetning, at Datatilsynet i forlængelse af fastsættelsen af de omtalte vilkår gjorde opmærksom på, at vilkårene er supplerende i forhold til reglerne i persondataloven samt i visse tilfælde udtryk for en præcisering af lovens regler. Det blev derfor understreget, at reglerne i persondataloven finder anvendelse i det omfang, der er tale om forhold, som ikke er reguleret i vilkårene.

Datatilsynets praksis er endvidere omtalt i persondataloven med kommentarer[309], hvoraf det fremgår, at oplysninger, som ikke er fortrolige, principielt kan videregives uden nogen form for anonymisering. I den forbindelse er der henvist til Datatilsynets praksis om videregivelse af oplysninger gennem postlister, hvorefter der efter omstændighederne vil kunne ske offentliggørelse af postlister indeholdende ikke-følsomme oplysninger, herunder fortrolige oplysninger.[310]

3.13.3. Databeskyttelsesforordningen

Databeskyttelsesforordningen indeholder blandt andet grundlæggende behandlingsprincipper, jf. artikel 5, der ligner de gældende principper i persondatalovens § 5, og behandlingsbetingelser, der i vidt omfang svarer til de gældende. For eksempel følger det af forordningens artikel 6, at (ikke-følsomme) oplysninger kan behandles, hvis det er nødvendigt af hensyn til udførelse af en opgave i samfundets interesse, jf. artikel 6, stk. 1, litra e. Som noget nyt er det tilføjet i forordningens artikel 6, stk. 3, at grundlaget for behandling i henhold til den nævnte behandlingsbetingelse skal fremgå af enten EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt. Desuden følger det af bestemmelsen, at formålet med behandlingen skal være fastlagt i dette retsgrundlag eller for så vidt angår den behandling, der er omhandlet i stk. 1, litra e, være nødvendig for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, og at dette retsgrundlag kan indeholde specifikke bestemmelser med henblik på at tilpasse anvendelsen af bestemmelserne i denne forordning, bl.a. de generelle betingelser for lovlighed af den dataansvarliges behandling, hvilke typer oplysninger der skal behandles, berørte registrerede, hvilke enheder personoplysninger må videregives til og formålet hermed, formålsbegrænsninger, opbevaringsperioder og behandlingsaktiviteter samt behandlingsprocedurer, herunder foranstaltninger til sikring af lovlig og rimelig behandling såsom i andre specifikke databehandlingssituationer som omhandlet i forordningens kapitel IX. EU-retten eller medlemsstaternes nationale ret

[309] Persondataloven med kommentarer (2015), s. 324 ff.
[310] Persondataloven med kommentarer (2015), s. 244 nederst f.

skal opfylde et formål i samfundets interesse og stå i rimeligt forhold til det legitime mål, der forfølges.

Desuden følger det af forordningens artikel 6, stk. 2, at medlemsstaterne kan opretholde eller indføre mere specifikke bestemmelser for at tilpasse anvendelsen af denne forordnings bestemmelser om behandling med henblik på overholdelse af bl.a. stk. 1, litra e, ved at fastsætte mere præcist specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling, herunder for andre specifikke databehandlingssituationer som omhandlet i forordningens kapitel IX.

Behandlingen af følsomme oplysninger er reguleret i databeskyttelsesforordningens artikel 9. Ifølge bestemmelsens stk. 1 er det forbudt at behandle personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Ifølge artikel 9, stk. 2, litra g, finder bestemmelsen i stk. 1 ikke anvendelse, hvis behandling er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Herudover følger det bl.a. af betragtning nr. 10 til forordningen, at medlemsstaterne i forbindelse med behandling af personoplysninger, for bl.a. at udføre en opgave i samfundets interesse, bør kunne opretholde eller indføre nationale bestemmelser for yderligere at præcisere anvendelsen af denne forordnings bestemmelser, og at medlemsstaterne sammen med generel og horisontal lovgivning om databeskyttelse til gennemførelse af databeskyttelsesdirektivet har flere sektorspecifikke love på områder, hvor der er behov for mere specifikke bestemmelser, samt at forordningen også indeholder en manøvremargen, så medlemsstaterne kan præcisere reglerne heri, herunder for behandling af særlige kategorier af personoplysninger ("følsomme oplysninger"). Hertil fremgår det, at forordningen således ikke udelukker, at medlemsstaternes nationale ret fastlægger omstændighederne i forbindelse med specifikke databehandlingssituationer, herunder mere præcis fastlægger de forhold, hvorunder behandling af personoplysninger er lovlig.

3.13.4. Overvejelser

Databeskyttelsesforordningen indeholder regler, som i vidt omfang svarer til reglerne i det gældende direktivs artikel 5 og 8, stk. 4, og som dermed må antages på samme måde som i dag at give medlemsstaterne mulighed for at fastsætte nærmere regler under forudsætning af, at der gives tilstrækkelige garantier, der præciserer reglerne i forordningen.

Det må derfor antages, at det er muligt at videreføre en bestemmelse svarende til persondatalovens § 9, når forordningen får virkning 25. maj 2018.

4. Forordningens kapitel III: Den registreredes rettigheder

4.1. Gennemsigtig oplysning, artikel 12

4.1.1. Præsentation

Forordningens artikel 12 indeholder en række generelle betingelser for, hvordan den dataansvarlige skal kommunikere, når der skal ske opfyldelse af de oplysningspligter, der følger af artikel 13 og 14, og hvordan der skal kommunikeres omkring artikel 15–22 samt artikel 34.

4.1.2. Gældende ret

Der er ikke i gældende ret en specifik bestemmelse, der generelt fastsætter, hvordan den dataansvarlige skal kommunikere med den registrerede.

Det følger af persondatalovens § 31, stk. 1, at såfremt den registrerede ønsker indsigt i de oplysninger, der eventuelt behandles af en dataansvarlig, skal den dataansvarlige, såfremt der behandles oplysninger, give den registrerede meddelelse på en *let forståelig måde*. Samme krav følger af persondatalovens § 22, stk. 1, der vedrører retten til indsigt i kreditoplysningsbureauers oplysninger. Den registreredes indsigtsret baserer sig på artikel 12 i databeskyttelsesdirektivet.

Det må afhænge af den konkrete situation, hvad der nærmere ligger i kravet om en *let forståelig måde*. Grundlæggende må det være et krav, at meddelelsen gives i en sådan form og på en sådan måde, at den registrerede er i stand til at forstå indholdet af de pågældende oplysninger og bedømmelser.[311] Dette krav må antageligvis også betyde, at den dataansvarlig skal kommunikere i et sprog, som er til at forstå for den registrerede uanset dennes alder. I modsat fald ville opfyldelse af registreredes rettigheder ikke være effektiv.

Persondatalovens § 34 foreskriver, at meddelelser i henhold til persondatalovens § 31, stk. 1, om ret til indsigt som udgangspunkt skal gives skriftligt, hvis den registrerede anmoder herom. Derudover følger det af bestemmelsen, at i de tilfælde, hvor hensynet til den registrerede taler herfor, kan meddelelse af indsigt ske i form af en mundtlig underretning om indholdet af oplysningerne. Dette vil bl.a. kunne være tilfældet med hensyn til oplysning om den registreredes helbredsforhold. Det følger af bemærkningerne til persondatalovens § 34, at oplysningerne, såfremt de gives skriftligt, skal fremtræde i en sådan form, at de kan læses umiddelbart og uden brug af tekniske hjælpemidler.

[311] Persondataloven med kommentarer (2015), s. 394.

4.1.3. Databeskyttelsesforordningen

4.1.3.1. Databeskyttelsesforordningens artikel 12, stk. 1

Det fremgår af forordningens artikel 12, stk. 1, at den dataansvarlige skal træffe passende foranstaltninger til at give enhver oplysning som omhandlet i artikel 13 og 14 og enhver meddelelse i henhold til artikel 15–22 og 34 om behandling til den registrerede i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog, navnlig når oplysninger specifikt er rettet mod et barn. Oplysningerne gives skriftligt eller med andre midler, herunder, hvis det er hensigtsmæssigt, elektronisk. Når den registrerede anmoder om det, kan oplysninger gives mundtligt, forudsat at den registreredes identitet godtgøres med andre midler.

Artikel 12, stk. 1, suppleres af præambelbetragtning nr. 58, der fastsætter nærmere om princippet om gennemsigtighed. Heraf fremgår det, at dette gælder ved enhver oplysning, som er rettet til offentligheden eller den registrerede, og at sådanne oplysninger kan gøres tilgængelige i elektronisk form. Dette vil især være relevant, når det – af hensyn til den anvendte teknologis kompleksitet – er vanskeligt for den registrerede at vide og forstå, om, af hvem og til hvilket formål der indsamles personoplysninger om vedkommende. Med udspecificeringen af oplysninger, der er rettet til et barn, menes, at sprogbruget skal være så enkelt og klart, at et barn let kan forstå det.

Det følger af kravet i artikel 12, stk. 1, om, at oplysninger gives til den registrerede, at oplysningspligten ikke kan opfyldes ved, at den dataansvarlige på en hjemmeside eller lignende informerer i overensstemmelse med oplysningspligten, da den registrerede dermed ikke gives oplysninger.

Det følger af formkravet i artikel 12, stk. 1, at oplysningerne gives elektronisk, hvis det er *hensigtsmæssigt*. Af forordningens artikel 12, stk. 3, følger det, at hvis den registrerede indgiver en anmodning elektronisk, meddeles oplysninger *så vidt muligt* elektronisk. Hensigtsmæssighedskravet i stk. 1, kan indeholdes i kravet om *så vidt muligt* i stk. 3, i og med, at det oftest vil være hensigtsmæssigt at give oplysninger elektronisk, hvis den registrerede indgiver en anmodning elektronisk. Derudover vil det kunne undlades i de situationer, hvor det ikke er hensigtsmæssigt at meddele oplysningerne elektronisk, da der med *så vidt muligt* er taget højde for, at oplysninger ikke altid kan meddeles elektronisk.

Det bemærkes i den forbindelse, at det ved lov kan være bestemt, at det offentlige er berettiget til at kommunikere elektronisk med borgerne, jf. f.eks. lov om Digital Post.

Databeskyttelsesforordningens artikel 12, stk. 1, præciserer og tydeliggør de formkrav, som den dataansvarlige er underlagt, når der skal gives oplysninger eller meddelelse. Selv-

om der ikke er en direkte bestemmelse i gældende ret, som svarer til forordningens artikel 12, stk. 1, vil der antageligvis ikke være tale om, at artikel 12, stk. 1, medfører en væsentligt ændret retstilstand.

4.1.3.2. Databeskyttelsesforordningens artikel 12, stk. 2

Det fremgår af forordningens artikel 12, stk. 2, 1. pkt., at den dataansvarlige letter udøvelsen af den registreredes rettigheder i henhold til artikel 15-22. Oplysningspligten i artikel 13-14 nævnes ikke i artikel 12, stk. 2.

Artikel 12, stk. 2, suppleres af præambelbetragtning nr. 59, hvoraf det fremgår, at der med at *lette udøvelsen* bl.a. tænkes på mekanismer til at anmode om indsigt i og berigtigelse eller sletning af personoplysninger og udøvelsen af retten til indsigt. Derudover bør den dataansvarlige give mulighed for elektroniske anmodninger, navnlig hvis personoplysninger behandles elektronisk. Et eksempel kunne være, at en digital tjeneste udvikler et tydeligt ikon på sin hjemmeside, hvor brugerne nemt kan anmode tjenesten om indsigt, berigtigelse eller sletning af personoplysninger.

Det er den registrerede, der skal udøve de rettigheder, der følger af artikel 15–22. Udøvelsen sker således på den registreredes initiativ. Den dataansvarlige kan *lette* denne udøvelse ved aktivt at gøre opmærksom på rettighedernes eksistens eller ved at sikre sig, at der er etableret systemer, der kan modtage og behandle henvendelser fra registrerede på en måde, der ikke er unødigt besværlig og som sikrer den registreredes rettigheder.

Af den engelske sprogversion følger det, at den dataansvarlige skal "*facilitate* the exercise of data subject rights". På dansk kan dette også oversættes til facilitering, hvilket betyder at gøre noget svært muligt eller lettere.

Det fremgår af forordningens artikel 12, stk. 2, 2. pkt., at i de tilfælde, der er omhandlet i artikel 11, stk. 2, må den dataansvarlige ikke afvise at efterkomme den registreredes anmodning om at udøve sine rettigheder i henhold til artikel 15-22, medmindre den dataansvarlige påviser, at vedkommende ikke er i stand til at identificere den registrerede.

For en gennemgang af de tilfælde, der er omhandlet i artikel 11, stk. 2, henvises til afsnit 3.12. om behandling, der ikke kræver identifikation.

Med bestemmelsen tænkes altså på en situation, hvor den registrerede har kontaktet den dataansvarlige for at udøve en rettighed, men hvor den dataansvarlige på baggrund af denne henvendelse – eller i øvrigt – ikke kan identificere den registrerede. Hvis den dataansvarlige da kan påvise, at den registrerede ikke kan identificeres, kan den registreredes

anmodning afvises. Såfremt den dataansvarlige ved en senere anmodning fra den registrerede, f.eks. fordi den registrerede som svar på afvisningen fra den dataansvarlige giver tilstrækkelige oplysninger til at identifikation er mulig, kan anmodningen ikke længere afvises på baggrund af artikel 12, stk. 2, 2. pkt.

Der vil antageligvis ikke være tale om, at artikel 12, stk. 2, medfører en ændret retstilstand, idet det væsentligt må følge af de krav, der stilles til den dataansvarlige om den registreredes rettigheder efter persondataloven, at den dataansvarlige skal sikre den registrerede muligheder for udøvelsen af sådanne rettigheder.

4.1.4. Overvejelser

Med databeskyttelsesforordningens artikel 12, stk. 1 og 2, sker der en præcisering og tydeliggørelse af de formkrav, som den dataansvarlige er underlagt, når der skal gives oplysninger eller meddelelse i forbindelse med registreredes udøvelse af deres rettigheder efter forordningen. Allerede i dag må dataansvarlige antages at skulle kommunikere på en måde og i et sprog, som er til at forstå for den registrerede uanset dennes alder, hvorfor der er tale om en videreførelse af gældende ret.

4.2. Processuelle spørgsmål om registreredes rettigheder, artikel 12, stk. 3-8

4.2.1. Præsentation

I databeskyttelsesforordningens artikel 12, stk. 3-8, fastsættes en række nærmere (processuelle) regler for udøvelsen af de registreredes rettigheder.

Nogle af reglerne er umiddelbart kendt fra persondataloven og databeskyttelsesdirektivet, mens andre er helt nye.

Endvidere er nogle af reglerne, for så vidt angår offentlige myndigheder, kendt fra forvaltningsloven og fra de ulovbestemte principper om god forvaltningsskik.

4.2.2. Gældende ret

De gældende generelle persondataretlige regler om de registreredes rettigheder findes i persondatalovens afsnit III (kapitel 8-10)[312] og i regler udstedt i medfør deraf.[313]

[312] Der findes også mere specielle regler, som f.eks. oplysningspligt på kreditoplysningsområdet i persondatalovens kapitel 6 og i persondatalovens § 36 om markedsføring.
[313] Bekendtgørelse nr. 530 af 15. juni 2000 om betaling for skriftlige meddelelser fra kreditoplysningsbureauer og bekendtgørelse nr. 533 af 15. juni 2000 om betaling for private dataansvarliges skriftlige meddelelser om indsigt.

Herudover er nogle af reglerne i databeskyttelsesforordningens artikel 12, stk. 3-8, som nævnt ovenfor, kendt fra forvaltningsloven og fra de ulovbestemte principper om god forvaltningsskik.

4.2.2.1. Frist for besvarelse af anmodninger fra de registrerede

4.2.2.1.1. Frister der følger af persondataloven

Af persondatalovens § 31, stk. 2, fremgår det, at den dataansvarlige snarest skal besvare begæringer om indsigt fra de registrerede. Det fremgår tillige, at den dataansvarlige, hvis begæringen ikke er besvaret inden 4 uger efter modtagelsen, skal underrette den pågældende om grunden hertil, samt om, hvornår afgørelsen så kan forventes at foreligge.

Om persondatalovens § 31, stk. 2, fremgår det af bemærkningerne[314] til loven, at den tid, der vil hengå med at ekspedere en anmodning om indsigt, vil kunne variere afhængig af, hvilken form for behandling der er tale om. Det fremgår endvidere af bemærkningerne, at den dataansvarlige i mange tilfælde først vil kunne meddele indsigt, når oplysningerne er rekvireret hos en databehandler. Herudover fremgår det af bemærkningerne, at ekspeditionstidens længde vil være afhængig af den tekniske indretning af det system, hvori oplysningerne behandles. Der er derfor, ifølge bemærkningerne til loven, ikke fastsat nogen absolut frist. I stedet er der i bestemmelsens 2. pkt. indsat en regel, hvorefter en dataansvarlig, hvis det undtagelsesvis tager længere tid end 4 uger at behandle en begæring om indsigt, skal underrette den registrerede herom. Endelig fremgår det af bemærkningerne, at underretningen af den registrerede skal indeholde oplysninger om grunden til, at der ikke kan træffes afgørelse inden for 4 ugers fristen, samt om, hvornår en afgørelse vil foreligge.

Af afsnit 3.3. i Datatilsynets vejledning om de registreredes rettigheder[315] fremgår det endvidere, at mindre og ukomplicerede indsigtsbegæringer skal besvares hurtigt (snarest muligt), og at den dataansvarlige ikke blot vil kunne vente med at besvare en sådan begæring ved udløbet af 4 ugersfristen. Omvendt skal fristen for besvarelse af omfattende begæringer om indsigt fastsættes under rimelig hensyntagen hertil. Dog må den tid, der går med at besvare begæringer om indsigt aldrig overstige den tidsmæssige ramme i artikel 12, litra a, i databeskyttelsesdirektivet, hvoraf det fremgår, at indsigtsbegæringer skal besvares "uden større ventetid".

Samme sted i vejledningen fremgår det, at bemærkningerne til § 31, stk. 2, skal forstås således, at det i de tilfælde, hvor der er tale om behandlinger, der ajourføres løbende, og

[314] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 31.

[315] Vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger.

hvor udtræk sker i forbindelse med sådanne ajourføringer, normalt vil være i overensstemmelse med bestemmelsen i stk. 2 at udtrække oplysningerne i forbindelse med den førstkommende ajourføring af de behandlede oplysninger, hvis ajourføringen sker månedligt eller med kortere mellemrum. Hvis behandlingerne derimod ikke sker månedligt eller med kortere mellemrum, vil en længere svarfrist end 4 uger kun efter omstændighederne være acceptabel i en overgangsperiode, indtil registret bliver indrettet til en hyppigere ajourføring.

Endelig fremgår det, at en dataansvarlig altid har mulighed for – men ikke pligt til – at besvare begæringer om indsigt løbende. Denne løsning vil f.eks. med fordel kunne benyttes af en kommune, hvor flere forskellige kontorer og forvaltninger kan behandle oplysninger om en person.

4.2.2.1.2. Frister der følger af princippet om god forvaltningsskik (offentlige myndigheder)
I Danmark suppleres forvaltningslovens regler af en række uskrevne forvaltningsprocessuelle grundsætninger samt af principperne om god forvaltningsskik.[316]

Ombudsmanden har således i en lang række sager med offentlige myndigheder udviklet retsgrundsætninger og principper om god forvaltningsskik for behandlingen af sager, der ikke har karakter af afgørelsessager. Det samme gør sig også gældende i forhold til retsspørgsmål, hvor forvaltningsloven finder anvendelse, og hvor retsudviklingen af supplerende grundsætninger og god forvaltningsskik er fortsat efter forvaltningslovens vedtagelse.[317]

Et centralt tema for den gode forvaltningsskik har været og er myndighedernes sagsbehandlingstider og effektive sagsgange.[318]

I FOB 1988.290 har Folketingets Ombudsmand bl.a. udtalt følgende om sagsbehandlingstider: ”Bortset fra enkelte særregler som f.eks. forvaltningslovens § 16, stk. 2, er der ikke i lovgivningen fastlagt normer for, hvor længe forvaltningsmyndighederne må være om at behandle sagerne. Hvad der er acceptabel sagsbehandlingstid, må vurderes konkret under hensyn til, hvor mange ekspeditioner en forsvarlig oplysning af sagen kræver, om der foreligger faktiske hindringer for ekspeditionerne, om særlige tidskrævende undersøgelser er påkrævet, om sagen efter sin art er hastende samt forholdet mellem myndighedernes ressourcer og arbejdsopgaver […].”

[316] Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave (2013), s. 55.
[317] Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave (2013), s. 56.
[318] Hans Gammeltoft-Hansen m.fl., Forvaltningsret, 2. udgave (2002), s. 622 ff.

Der er således også allerede i dag en grænse for, hvor længe en myndighed må være om at behandle f.eks. en anmodning fra en registreret om berigtigelse af oplysninger om den pågældende selv i medfør af persondatalovens § 37. Grænsen ligger dog ikke fast, men kan – efter klage fra den registrerede – bedømmes konkret i den enkelte sag af Folketingets Ombudsmand med udgangspunkt i bl.a. ovennævnte kriterier.

4.2.2.2. Begrundelse og klagevejledning til de registrerede

Som nævnt ovenfor findes de gældende generelle persondataretlige regler om de registreredes rettigheder i persondatalovens afsnit III (kapitel 8-10).

Ingen af disse regler indeholder bestemmelser om begrundelse og klagevejledning ved manglende imødekommelse af en anmodning fra de registrerede.

Af bemærkningerne[319] til persondatalovens § 35 fremgår det bl.a., at den indsigelsesret, der tilkommer de registrerede efter stk.1, har den virkning, at en forvaltningsmyndigheds beslutning om, hvorvidt en indsigelse skal imødekommes, har karakter af en afgørelse efter forvaltningsloven. Dette indebærer, at myndigheden skal overholde forvaltningslovens regler om begrundelse, klagevejledning mv.

Endvidere fremgår det af persondataloven med kommentarer[320], at meget taler for, at det samme gør sig gældende med hensyn til persondatalovens § 37 og formentlig også de øvrige rettigheder, der tilkommer de registrerede efter persondatalovens kapitel 10.

Som følge af ovennævnte skal offentlige dataansvarlige allerede i dag, efter forvaltningslovens kapitel 6 og 7, give en begrundelse for sine afgørelser efter reglerne i persondatalovens kapitel 10, ligesom den offentlige dataansvarlige vil skulle give klagevejledning[321], når dennes afgørelse ikke giver den registrerede fuldt ud medhold.

4.2.2.3. Opkrævning af gebyr ved opfyldelse af indsigtsbegæringer og imødekommelse af anmodninger fra de registrerede

Af § 1, stk. 1, i bekendtgørelse nr. 533 af 15. juni 2000 om betaling for private dataansvarliges skriftlige meddelelser om indsigt[322] fremgår det, at en privat dataansvarlig – i forbindelse med imødekommelse af en anmodning om indsigt fra en registreret – kan kræve 10 kr. for hver påbegyndt side, men dog maksimalt 200 kr. i alt.

[319] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 35.
[320] Persondataloven med kommentarer (2015), s. 519 ff.
[321] Om muligheden for at påklage afgørelsen til en anden forvaltningsmyndighed eller indbringe afgørelsen for domstolene, hvis afgørelsen ikke kan påklages til en anden myndighed.
[322] Udstedt i medfør af persondatalovens § 34, stk. 2

Det fremgår desuden af § 1, stk. 2, at hvis en person har forlangt, at en privat dataansvarlig giver skriftlig meddelelse om, at der ikke behandles oplysninger om den pågældende person, kan den private dataansvarlige kræve 10 kr. i betaling derfor.

Af § 1, stk. 3, fremgår det, at de efter stk. 1 og 2 opkrævne beløb omfatter merværdiafgift, forsendelsesomkostninger og lignende.

Omvendt kan den private dataansvarlige ikke kræve betaling fra den registrerede, hvis den registrerede ikke har forlangt, at besvarelsen af dennes henvendelse skal være skriftlig, jf. bekendtgørelsens § 2. Dette gælder også, selvom den dataansvarlige har meddelt indsigt i skriftlig form.[323]

For så vidt angår betaling for skriftlige meddelelser fra kreditoplysningsbureauer følger nogle næsten – i forhold til ovennævnte bekendtgørelse – identiske regler af bekendtgørelse nr. 530 af 15. juni 2000. Eneste undtagelse er, at kreditoplysningsbureauer som udgangspunkt ikke kan kræve betaling for den første meddelelse, der gives efter, at den, der behandles oplysninger om, har fået meddelelse efter persondatalovens § 21.

4.2.2.4. Afklaring af identitet ved besvarelse af anmodninger fra de registrerede
I afsnit 1.3. i føromtalte vejledning om de registreredes rettigheder[324] er spørgsmålet om afklaring af den registreredes identitet ved besvarelse af anmodninger fra denne nærmere beskrevet.

Af afsnit 1.3. i vejledningen fremgår det således, at persondataloven skal bl.a. sikre, at den enkelte borgers retsbeskyttelse og integritet ikke krænkes i forbindelse med den dataansvarliges behandling af personoplysninger. Herudover fremgår det af vejledningen, at i overensstemmelse hermed er det fastsat i lovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Det fremgår endvidere af vejledningen, at den dataansvarlige - og en eventuel databehandler - derfor skal sikre sig, at *den, der meddeles oplysninger til, er rette person*, så oplysninger om den registrerede ikke kommer til uvedkommendes kendskab. Der må, ifølge vejledningen, kun udleveres oplysninger, når vedkommende har legitimeret sig behørigt, eller

[323] Se side 13 i vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger.
[324] Vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger.

når der på anden måde er skabt sikkerhed for, at den, der f.eks. fremsætter en indsigtsbegæring, er identisk med den person, som oplysningerne vedrører.

Det fremgår desuden af vejledningen, at der ikke gælder specifikke regler for, hvorledes dette skal sikres, men sædvanlige legitimationspapirer, såsom pas, kørekort eller ID-kort mv., vil kunne kræves forevist. Navnlig i forbindelse med udlevering af fortrolige oplysninger, herunder særligt oplysninger om rent private forhold (f.eks. oplysninger om strafbare forhold samt oplysninger om helbredsforhold og væsentlige sociale problemer), er det vigtigt at sikre, at oplysningerne ikke udleveres til uvedkommende.

Det fremgår endvidere af vejledningen, at kravet om legitimation kan fraviges, når der på anden måde er skabt sikkerhed for, at den person, som f.eks. fremsætter en begæring om indsigt, er identisk med den person, oplysningerne vedrører. Herved tænkes navnlig på den situation, at den medarbejder hos den dataansvarlige, som modtager begæringen, i forvejen kender den person, der fremsætter begæringen. Herudover fremgår det af vejledningen, at når en henvendelse er fremsat skriftligt, og hvis navn og adresse i brevet er identisk med de oplysninger, som i forvejen fremgår af sagen, vil der i almindelighed ikke være grund til at foretage særlige undersøgelser, inden oplysningerne sendes til den registrerede på den angivne adresse. Herefter fremgår det af vejledningen, at såfremt dette ikke er tilfældet, bør forholdet undersøges nærmere, f.eks. ved at der rettes henvendelse til den person, der har fremsat begæringen eller til folkeregisteret, evt. via onlineadgang til Det Centrale Personregister (CPR). Særligt gælder det, ifølge vejledningen, at der bør udvises forsigtighed med fremsendelse af fortrolige oplysninger til en c/o-adresse, som den registrerede ikke selv har oplyst.

For så vidt angår elektroniske henvendelser, f.eks. i form af en e-post, der er forsynet med en elektronisk signatur med tilhørende kvalificeret certifikat, fremgår det af vejledningen, at disse må antages at kunne sidestilles med skriftlige henvendelser, såfremt den elektroniske signatur og det medfølgende kvalificerede certifikat opfylder kravene i lov nr. 417 af 31. maj 2000 om elektronisk signatur. Der vil således heller ikke her - i tilfælde hvor navn og adresse i den elektroniske henvendelse er identisk med de oplysninger, som i forvejen fremgår af sagen - i almindelighed være grund til at foretage særlige undersøgelser, inden oplysningerne sendes til den registrerede på den angivne postadresse.

Det fremgår endvidere af vejledningen, at der ved telefoniske henvendelser og ved elektroniske henvendelser i form af en e-post, der ikke er forsynet med elektronisk signatur med tilhørende kvalificeret certifikat, ligeledes skal træffes de fornødne sikkerhedsforanstaltninger for, at der kun udleveres oplysninger til de rette personer. Det kan f.eks. være nødvendigt at foretage en kontrolopringning.

Det fremgår desuden af vejledningen, at de registrerede personer i en række offentlige registre ikke vil være identificeret ved navn og adresse, men ved personnummer, ligesom personnummeret ofte vil være »indgangsnøgle« til registeret. I disse tilfælde kan personen opfordres til at oplyse sit personnummer tillige med navn og adresse. Såfremt vedkommende ikke ønsker at oplyse personnummeret, vil dette, ifølge vejledningen, imidlertid ikke i sig selv være tilstrækkeligt grundlag for at meddele afslag på f.eks. en indsigtsbegæring. Hvis det af praktiske grunde er nødvendigt for myndigheden at søge det oplyst, må myndigheden i sådanne tilfælde søge personnummeret oplyst på anden måde, f.eks. via onlineadgang til Det Centrale Personregister (CPR).

Omvendt er det, ifølge vejledningen, ikke tilstrækkelig legitimation, at en person ved personligt fremmøde eller ved telefonisk henvendelse er i stand til at oplyse en registreret persons personnummer. Her skal det på anden måde sikres, at den pågældende er identisk med den registrerede eller på andet grundlag, f.eks. en fuldmagt, har lovlig adkomst til oplysningerne. Det gælder med andre ord, at *hverken offentlige myndigheder eller private virksomheder mv. må basere sin datasikkerhed på personnummeret som en form for adgangskode (password)*.

Endelig fremgår det af vejledningen, hvis den dataansvarlige har etableret adgang til at søge indsigt i behandlede oplysninger gennem et elektronisk selvbetjeningssystem, f.eks. via en hjemmeside, påhviler der den dataansvarlige en pligt til at sikre, at uvedkommende ikke kan få adgang til oplysningerne. Også her gælder det naturligvis, ifølge vejledningen, at adgangen til indsigt i oplysninger om den enkelte ikke må baseres på personnummeret som adgangskode (password).

Ligeledes vil det være tilstrækkeligt sikkert, hvis en offentlig dataansvarlig f.eks. besvarer en indsigtsanmodning ved at sende oplysningerne via postløsningen Digital Post.[325] Det samme gør sig gældende for private dataansvarlige, der benytter sig af løsningen.

4.2.3. Databeskyttelsesforordningen

4.2.3.1. Databeskyttelsesforordningens artikel 12, stk. 3

Det fremgår af databeskyttelsesforordningens artikel 12, stk. 3, at den dataansvarlige uden unødig forsinkelse og i alle tilfælde senest en måned efter modtagelsen af anmodningen oplyser den registrerede om foranstaltninger, der træffes på baggrund af en anmodning i henhold til artikel 15-22.[326]

[325] Se mere herom i lovbekendtgørelse nr. 801 af 13. juni 2016 om digital post fra offentlige afsendere.

[326] Databeskyttelsesforordningens artikel 15-22 indeholder regler om indsigtsret, ret til berigtigelse, ret til sletning, ret til begrænsning af behandling, underretningspligt ved bl.a. berigtigelse, ret til dataportabilitet, ret til indsigelse og automatiske individuelle afgørelser.

Endvidere fremgår det, at ovennævnte periode kan forlænges med to måneder, hvis det er nødvendigt under hensyntagen til anmodningernes kompleksitet og antal.[327]

Hvis perioden forlænges, fremgår det desuden af artikel 12, stk. 3, at den dataansvarlige skal underrette den registrerede om enhver sådan forlængelse senest en måned efter modtagelsen af anmodningen sammen med en begrundelse for forsinkelsen.

Endelig fremgår det af bestemmelsen, at hvis den registrerede indgiver en anmodning elektronisk, meddeles oplysningerne så vidt muligt elektronisk, medmindre den registrerede anmoder om andet.

Af præambelbetragtning nr. 59 fremgår det, at der bør fastsættes nærmere regler, som kan lette udøvelsen af de registreredes rettigheder i henhold til denne forordning, herunder mekanismer til at anmode om og i givet fald opnå navnlig gratis indsigt i og berigtigelse eller sletning af personoplysninger og udøvelsen af retten til indsigelse. Det fremgår endvidere, at den dataansvarlige bør være forpligtet til at besvare anmodninger (i forbindelse med udøvelsen af de registreredes rettigheder) fra en registreret uden unødig forsinkelse og senest inden for en måned og begrunde det, hvis vedkommende ikke agter at imødekomme sådanne anmodninger. Herudover fremgår det, at den dataansvarlige bør give mulighed for elektroniske anmodninger, navnlig hvis personoplysninger behandles elektronisk.

For så vidt angår de dataansvarliges besvarelse af anmodninger om indsigt, ligner databeskyttelsesforordningens artikel 12, stk. 3, i vidt omfang de gældende regler i persondatalovens § 31, stk. 2, sammenholdt med databeskyttelsesdirektivets artikel 12.

Nyt er det imidlertid, at den periode, hvormed svarfristen i visse situationer kan forlænges, udtrykkeligt fastsættes til maksimalt to måneder, hvor der i dag ikke er nogen absolut frist. Den nye absolutte forlængelsesfrist på to måneder medfører dog næppe en ændring af gældende ret, idet det må antages, at der heller ikke i dag vil forekomme situationer, hvor en dataansvarlig kan komme med en legitim begrundelse for, at det skal tage mere end i alt tre måneder at besvare en anmodning om indsigt.

Det, at det fremgår af artikel 12, stk. 3, at en elektronisk anmodning om udnyttelse af én af de registreredes rettigheder, jf. artikel 15-22, fra den registrerede, så vidt muligt, skal besvares elektronisk, må ligeledes antages at være en videreførelse af gældende ret for så vidt angår offentlige dataansvarlige, idet man i Danmark allerede på nuværende tidspunkt, i videst muligt omfang, kommunikerer elektronisk med borgere og virksomheder, jf. bl.a.

[327] Der kan måske findes inspiration i gennemgangen af offentlighedslovens § 36 i Mohammad Ahsan, Offentlighedsloven med kommentarer, 1. udgave (2014), s. 638 ff.

den fællesoffentlige digitaliseringsstrategi for 2011-2015.[328] For private dataansvarlige er kravet en nyskabelse.

I forhold til de registreredes øvrige rettigheder[329] er det derimod nyt, at anmodninger fra de registrerede skal besvares lige så hurtigt som anmodninger om indsigt. Dette nye krav vil formentlig medføre et behov for, at private dataansvarlige fastsætter nærmere rutiner for besvarelse af alle de registreredes anmodninger. Et lignende behov for nye rutiner – eller indarbejdelse i nuværende – vil formentlig også gøre sig gældende i forhold til offentlige dataansvarlige, selvom disse i dag er underlagt de ulovbestemte krav om sagsbehandlingstider, der følger af god forvaltningsskik. Baggrunden herfor er, at den tidsfrist, der fremgår af databeskyttelsesforordningens artikel 12, stk. 3, i de fleste tilfælde må antages at være kortere end den frist, der i en konkret sag måtte følge af princippet om god forvaltningsskik.

4.2.3.2. Databeskyttelsesforordningens artikel 12, stk. 4

Af databeskyttelsesforordningens artikel 12, stk. 4, fremgår det, at hvis den dataansvarlige ikke træffer foranstaltninger i anledning af den registreredes anmodning, underretter den dataansvarlige straks og senest en måned efter modtagelsen af anmodningen den registrerede om årsagen hertil og om muligheden for at indgive klage til en tilsynsmyndighed og indbringe sagen for en retsinstans.

For så vidt angår offentlige dataansvarlige ses den nye regel i databeskyttelsesforordningens artikel 12, stk. 4, i vidt omfang at være en videreførelse af gældende ret, idet offentlige dataansvarlige allerede i dag er omfattet af forvaltningslovens regler om begrundelse og klagevejledning, jf. gennemgangen heraf ovenfor. Dog er det nyt, at alle offentlige dataansvarlige vil skulle oplyse om muligheden for at indbringe en sag for domstolene. Dette yderligere krav vil kræve tilpasning af eventuelle standardformuleringer hos myndighederne.

Med hensyn til private dataansvarlige er det derimod nyt, at disse nu får en retlig forpligtelse til at begrunde eventuelle afslag på anmodninger fra de registrerede samt at give de registrerede klagevejledning som nævnt ovenfor. Private dataansvarlige begrunder allerede i dag i en række tilfælde deres afslag på anmodninger fra de registreredes, ligesom de i visse tilfælde vil give klagevejledning. I disse tilfælde vil det derfor kun være af mindre praktisk betydning, at de med databeskyttelsesforordningen bliver pålagt en retlig forpligtelse til at begrunde afslag og give klagevejledning.

[328] Se nærmere på Digitaliseringsstyrelsens hjemmeside.
[329] Databeskyttelsesforordningens artikel 16-22.

4.2.3.3. Databeskyttelsesforordningens artikel 12, stk. 5

Det fremgår af databeskyttelsesforordningens artikel 12, stk. 5, at oplysninger, der gives i henhold til artikel 13 og 14[330], og enhver meddelelse og enhver foranstaltning, der træffes i henhold til artikel 15-22 og 34[331], er gratis.

Herudover fremgår det af bestemmelsen, at den dataansvarlige, hvis anmodninger fra en registreret er åbenbart grundløse eller overdrevne, især fordi de gentages, enten kan:

a) Opkræve et rimeligt gebyr under hensyntagen til de administrative omkostninger ved at give oplysninger eller meddelelser eller træffe den ønskede foranstaltning, eller

b) afvise at efterkomme anmodningen.

Endelig fremgår det af artikel 12, stk. 5, at det er den dataansvarlige, der har bevisbyrden for, at en anmodning er åbenbart grundløs eller overdreven.

I lighed med gældende ret er udgangspunktet i databeskyttelsesforordningens artikel 12, stk. 5, at de dataansvarliges opfyldelse af deres oplysningspligt samt besvarelse af anmodninger fra de registrerede er gratis.

For så vidt angår de dataansvarliges opfyldelse af deres oplysningspligt[332] medfører databeskyttelsesforordningens artikel 12, stk. 5, ingen ændringer i forhold til gældende ret, da det hverken i dag, eller fra når forordningen finder anvendelse, vil være muligt at opkræve gebyrer eller at afvise at efterkomme oplysningspligten.

I forhold til private dataansvarlige, da vil disse med databeskyttelsesforordningens artikel 12, stk. 5, på den ene side få udvidet deres adgang til at opkræve gebyrer, da muligheden for at opkræve gebyrer ikke længere vil være begrænset til situationer, hvor den registrerede har anmodet om indsigt, men også vil gælde ved besvarelse af andre anmodninger fra de registrerede, jf. databeskyttelsesforordningens artikel 15-22 og 34. Hertil kommer, at der ikke længere vil være et loft for gebyrer på 200 kr. ved besvarelse af indsigtsanmodninger. Gebyrerne skal dog fortsat være rimelige under hensyntagen til de administrative omkostninger, hvorfor gebyrerne ikke kan fastsættes frit. På den anden side bliver de private dataansvarliges mulighed for at opkræve gebyrer, ved besvarelse af anmodninger om indsigt fra de registrerede, begrænset til situationer, hvor anmodningerne om indsigt er åbenbart

[330] Databeskyttelsesforordningens artikel 13 og 14 indeholder regler om den dataansvarliges oplysningspligt.
[331] Databeskyttelsesforordningens artikel 34 indeholder regler om underretning af den registrerede ved brud på persondatasikkerheden.
[332] Persondatalovens § 28-30 og databeskyttelsesforordningens artikel 13 og 14.

grundløse eller overdrevene (især fordi de gentages). I dag gælder der ikke et sådan krav efter bekendtgørelse om betaling for private dataansvarliges skriftlige meddelelser om indsigt.[333]

For offentlige dataansvarlige indebærer databeskyttelsesforordningens artikel 12, stk. 5, en ændring af gældende ret, da offentlige dataansvarlige nu får mulighed for at opkræve gebyrer i samme omfang som private dataansvarlige – det vil sige når anmodninger fra de registrerede er åbenbart grundløse eller overdrevene (især fordi de gentages). I praksis kan det især tænkes, at offentlige dataansvarlige vil overveje muligheden for at opkræve gebyrer i situationer, hvor en borger gang på gang anmoder om indsigt i de samme oplysninger – ofte med et chikanøst formål.

Det skal dog bemærkes, at der i almindelighed kræves lovhjemmel for, at en myndighed kan opkræve gebyrer for at udføre deres opgaver. Der henvises til afsnit 7.6. om åbenbart grundløse eller uforholdsmæssige anmodninger, artikel 57, stk. 4.

Det er i den forbindelse værd at bemærke, at databeskyttelsesforordningen ikke indeholder en regel svarende til persondatalovens § 33, hvorefter en registreret, der har fået indsigt, ikke har krav på at få indsigt på ny før 6 måneder efter sidste meddelelse af indsigt. Reglen i persondatalovens § 33 har hidtil været offentlige dataansvarliges eneste mulighed for at begrænse overdrevne anmodninger om indsigt fra de registrerede. Det fremgår dog af præambelbetragtning nr. 63, at en registreret bør have ret til indsigt i personoplysninger, der er indsamlet om vedkommende, og til let *med rimelige mellemrum* at udøve denne ret med henblik på at forvisse sig om og kontrollere en behandlings lovlighed

På baggrund af denne betragtning vil den registrerede, når databeskyttelsesforordningen får virkning, herefter have mulighed for at udøve sin indsigtsret med rimelige mellemrum. For nærmere om retten til indsigt, artikel 15, henvises til afsnit 4.5.

Herudover får alle dataansvarlige, som noget helt nyt, mulighed for at afvise anmodninger fra de registrerede, hvis anmodningerne er åbenbart grundløse eller overdrevne, især fordi de gentages. Umiddelbart må det antages, at de dataansvarlige vil være mere tilbøjelige til at anvende muligheden for at afvise en sag frem for at opkræve gebyrer. Dette skyldes, at det ofte vil være administrativt tungt at opkræve og inddrive gebyrer fra de registrerede. Ud over situationer, hvor en registreret kommer med overdrevne anmodninger om indsigt, kan muligheden for at afvise en sag også tænkes anvendt i situationer, hvor en registreret klager over, at samtlige oplysninger i den pågældendes sag hos en offentlig eller privat

[333] Bekendtgørelse nr. 533 af 15. juni 2000.

dataansvarlig er urigtige, men ikke – efter anmodning fra den dataansvarlige – ønsker at præcisere, hvilke oplysninger der er urigtige og med hvilken begrundelse. En sådan anmodning må efter omstændighederne kunne betragtes som åbenbart grundløs og/eller overdreven.

Det er vigtigt at være opmærksom på, at det efter artikel 12, stk. 5, er den dataansvarlige, der har bevisbyrden for, at en anmodning fra en registreret er åbenbart grundløs eller overdreven. En dataansvarlig, der ønsker at opkræve et gebyr eller afvise en sag under påberåbelse af denne bestemmelse, bør således sikre sig dokumentation for, at en anmodning fra en registreret er åbenbart grundløs eller overdreven. Denne dokumentation kan f.eks. bestå i, at den dataansvarlige gemmer alle anmodninger om indsigt fra en given registreret med henblik på at bevise, at antallet er overdreven mv.

Offentlige myndigheder bør også – når de overvejer at opkræve et gebyr eller afvise en sag – under påberåbelse af artikel 12, stk. 5, være opmærksom på den vejledningsforpligtelse, der følger af forvaltningslovens § 7, særligt når begrundelsen for f.eks. afvisningen er, at anmodningen fra den registrerede er overdreven. Den offentlige myndighed bør i disse situationer – i lighed med hvad der gælder i forhold til afvisninger i medfør af offentlighedslovens § 9, stk. 2[334] – indgå i en dialog med den registrerede med henblik på at få begrænset dennes anmodning, så den ikke længere er overdreven.

Endelig kan der henvises til gennemgangen af databeskyttelsesforordningens artikel 57, stk. 4, i afsnit om tilsynsmyndighedens opgaver, hvor en regel tilsvarende artikel 12, stk. 5, bliver beskrevet.

4.2.3.4. Databeskyttelsesforordningens artikel 12, stk. 6

Af artikel 12, stk. 6, i databeskyttelsesforordningen fremgår det, at den dataansvarlige, uden at det berører artikel 11, hvis der hersker rimelig tvivl om identiteten af den fysiske person, der fremsætter en anmodning som omhandlet i artikel 15-21, kan anmode om yderligere oplysninger, der er nødvendige for at bekræfte den registreredes identitet.

Det fremgår tillige af præambelbetragtning nr. 64, at den dataansvarlige bør træffe alle rimelige foranstaltninger for at bekræfte identiteten af en registreret, som anmoder om indsigt, navnlig i forbindelse med onlinetjenester og onlineidentifikatorer. Samtidig fremgår det dog også, at en dataansvarlig ikke bør opbevare personoplysninger alene for at kunne reagere på mulige anmodninger.

[334] Se mere herom i Mohammad Ahsan, Offentlighedsloven med kommentarer, 1. udgave (2014), s. 219 ff.

Databeskyttelsesforordningens artikel 12, stk. 6, må antages at være en videreførelse af gældende ret med hensyn til muligheden for at afklare de registreredes identitet ved besvarelse af anmodninger fra de disse.

4.2.3.5. Databeskyttelsesforordningens artikel 12, stk. 7 og 8

Det fremgår af databeskyttelsesforordningens artikel 12, stk. 7, at de oplysninger, der skal gives de registrerede i henhold til artikel 13 og 14, kan gives sammen med standardiserede ikoner for at give et meningsfuldt overblik over den planlagte behandling på en klart synlig, letforståelig og letlæselig måde. Hvis ikonerne præsenteres elektronisk, skal de være maskinlæsbare.

Stort set det samme, som fremgår af selve artikel 12, stk. 7, fremgår endvidere af præambelbetragtning nr. 60, sidste punktum.

Af databeskyttelsesforordningens artikel 12, stk. 8, fremgår det, at Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 92 med henblik på at fastlægge de oplysninger, der skal fremgå af standardiserede ikoner og procedurerne for tilblivelse af disse.

Om Kommissionens beføjelser fremgår det bl.a. af præambelbetragtning nr. 166, at Kommissionen navnlig bør vedtage delegerede retsakter om kriterier for og krav til certificeringsmekanismer, samt oplysninger, der skal fremgå af standardiserede ikoner, og procedurer for tilvejebringelse af sådanne ikoner. Samtidig fremgår det, at det er vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau. Kommissionen bør endvidere sikre samtidig, rettidig og hensigtsmæssig fremsendelse af relevante dokumenter til Europa-Parlamentet og til Rådet, når den forbereder og udarbejder delegerede retsakter.

Indholdet af databeskyttelsesforordningens artikel 12, stk. 7 og 8, er nyt i forhold til gældende ret.

Det må forventes, at Kommissionen vil benytte sig af sine beføjelser til at vedtage delegerede retsakter, og at Kommissionen i den forbindelse vil komme med en redegørelse for muligheden for brug af standardiserede ikoner ved de dataansvarliges opfyldelse af deres oplysningspligt over for de registrerede, jf. forordningens artikel 13 og 14.

4.2.4. Overvejelser

Databeskyttelsesforordningens artikel 12, stk. 3, er, for så vidt angår de dataansvarliges besvarelse af anmodninger om indsigt, i vidt omfang en videreførelse af gældende ret. Det

til trods for, at der, som noget nyt, indføres en maksimal forlængelsesfrist på to måneder, således at den absolutte frist for besvarelse af en indsigtsanmodning bliver på i alt tre måneder. Nyt er det derimod, at andre anmodninger fra de registrerede (berigtigelse, sletning mv.) skal besvares inden for samme frist som anmodninger om indsigt. Dette nye krav vil – i samspil med forordningens øvrige krav om dokumentation af efterlevelse[335] – formentlig medføre et behov for, at både private og offentlige dataansvarlige fastsætter nærmere rutiner for besvarelse af alle anmodninger fra de registrerede. For offentlige dataansvarlige gør behovet for rutiner sig gældende, selvom offentlige dataansvarlige allerede i dag er underlagt de ulovbestemte krav om sagsbehandlingstider, der følger af god forvaltningsskik. Nyt er det tillige, at en elektronisk anmodning fra en registreret, så vidt muligt, skal besvares elektronisk. Kravet må dog antages at være en videreførelse af gældende ret, idet man i Danmark allerede på nuværende tidspunkt, i videst muligt omfang, kommunikerer elektronisk med borgere og virksomheder.

Databeskyttelsesforordningens artikel 12, stk. 4, ses, for så vidt angår offentlige dataansvarlige, at være en videreførelse af gældende ret. Reglen er derimod en nyskabelse i forhold til private dataansvarlige, da disse nu får en retlig forpligtelse til at begrunde eventuelle afslag på anmodninger fra de registrerede samt til at give klagevejledning. I praksis er nyskabelsen dog formentlig af mindre betydning for private, da private dataansvarlige allerede i dag i en række tilfælde begrunder deres afslag på anmodninger fra de registrerede, ligesom de i visse tilfælde vil give klagevejledning.

Databeskyttelsesforordningens artikel 12, stk. 5, viderefører gældende rets udgangspunkt om, at de dataansvarliges opfyldelse af deres oplysningspligt samt besvarelse af anmodninger fra de registrerede er gratis. Dette gør sig altid gældende i forhold til de dataansvarliges opfyldelse af deres oplysningspligt, hvilket også er en videreførelse af gældende ret. Som noget nyt kan de dataansvarlige opkræve et rimeligt gebyr (under hensyntagen til de administrative omkostninger) ved besvarelse af alle anmodninger fra de registrerede, hvis anmodningerne er åbenbart grundløse eller overdrevne, især fordi de gentages. Tidligere har muligheden for gebyrer været forbeholdt private dataansvarlige, som har kunnet kræve op til 200 kr., hvis den registrerede har krævet en skriftlig besvarelse. Herudover får både offentlige og private dataansvarlige som noget nyt (alternativ til gebyr) mulighed for at afvise anmodninger fra de registrerede, hvis anmodningerne er åbenbart grundløse eller overdrevne, især fordi de gentages. Det er vigtigt at være opmærksom på, at det efter artikel 12, stk. 5, er den dataansvarlige, der har bevisbyrden for, at en anmodning fra en registreret er åbenbart grundløs eller overdreven.

[335] Bl.a. databeskyttelsesforordningens artikel 24.

Databeskyttelsesforordningens artikel 12, stk. 6, ses at være en videreførelse af gældende ret med hensyn til muligheden for at afklare de registreredes identitet ved besvarelse af anmodninger fra de disse.

Databeskyttelsesforordningens artikel 12, stk. 7 og 8, er nyskabelser i forhold til gældende ret. Det må forventes, at Kommissionen vil benytte sig af sine beføjelser til at vedtage delegerede retsakter, og at Kommissionen i den forbindelse vil komme med en redegørelse for muligheden for brug af standardiserede ikoner ved de dataansvarliges opfyldelse af deres oplysningspligt over for de registrerede, jf. forordningens artikel 13 og 14.

4.3. Oplysningspligt ved indsamling hos den registrerede, artikel 13

4.3.1. Præsentation

I persondatalovens § 28 er der fastsat en pligt til at meddele den registrerede oplysninger om en række forhold ved indsamling af personoplysninger hos denne.

Forordningens artikel 13 indeholder tilsvarende oplysningspligt ved indsamling af personoplysninger hos den registrerede.

4.3.2. Gældende ret

4.3.2.1. Persondatalovens § 28, stk. 1

Det fremgår af persondatalovens § 28, stk. 1, nr. 1-3, at den dataansvarlige eller dennes repræsentant ved indsamling af oplysninger hos den registrerede skal meddele den registrerede oplysninger om en række forhold. Denne bestemmelse er baseret på artikel 10 i databeskyttelsesdirektivet, der fastsætter en tilsvarende oplysningspligt ved oplysninger indsamlet hos den registrerede.

Det fremgår af præambelbetragtning nr. 38 i databeskyttelsesdirektivet, at en rimelig behandling forudsætter, at de registrerede kan få kendskab til en behandlings eksistens og, når der indsamles oplysninger hos dem, kan få nøjagtig og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen.

Det følger af bemærkningerne til persondataloven § 28, stk. 1, at bestemmelsen har til formål at sikre, at den registreredes beslutning om at afgive oplysninger om sig selv træffes på et pålideligt faktuelt grundlag med hensyn til en række forhold. Derudover følger det af bemærkningerne, at den dataansvarlige eller dennes repræsentant har pligt til af *egen drift* at give meddelelse til den registrerede, og at der intet krav gælder om, at meddelelsen skal

være skriftlig, men i og med, at den dataansvarlige skal kunne dokumentere, at meddelelsen er givet, anbefales det, at underretningen er skriftlig og tydelig.[336]

Persondatalovens § 30 fastsætter en række undtagelser til oplysningspligten i § 28.

Det følger af Datatilsynets vejledning om registreredes rettigheder efter reglerne i kapitel 8-10, at den dataansvarliges oplysningspligt indtræder over for den registrerede ved indsamling af oplysninger, og at den registrerede som udgangspunkt samtidig med indsamlingen skal have meddelelse om de i § 28 nævnte forhold. Derudover følger det af vejledningen, at der ikke gælder formkrav, og at den dataansvarlige alene er forpligtet til at give meddelelse til den registrerede én gang. Endelig følger det, at såfremt den registrerede selv henvender sig til den dataansvarlige, skal oplysningspligten, såfremt den er gældende, opfyldes snarest muligt, hvilket i almindelighed vil sige inden for 10 dage.[337]

Der er ikke i loven eller dens forarbejder taget stilling til, hvor udførlig underretningen af den registrerede skal være. Spørgsmålet afklares gennem tilsynsmyndighedernes praksis, hvor vægten lægges på, at formålet med reglen i § 28 er at sikre, at den registreredes beslutning om at afgive oplysninger om sig selv træffes på et pålideligt faktuelt grundlag med hensyn til en række nærmere beskrevne forhold, og at skabe større gennemsigtighed og overblik vedrørende personregistreringer. Af disse grunde, og da der ikke er et formkrav, må det stå den enkelte dataansvarlige forholdsvis frit med hensyn til at afgøre, hvorledes oplysningspligten skal opfyldes. Kravene til udførlighed må skulle afgøres i den konkrete situation under iagttagelse af de nævnte formål.[338]

Det følger af persondatalovens § 28, stk. 1, nr. 1, at der skal gives meddelelse om den dataansvarliges og dennes repræsentants identitet. En identisk bestemmelse følger af databeskyttelsesdirektivets artikel 10, litra a.

Det følger af bemærkningerne til persondataloven, at pligten til at give meddelelse om identitet kan opfyldes ved navn og adresse på den dataansvarlige og dennes eventuelle repræsentant. Det vil ikke være tilstrækkeligt, at der alene gives den registrerede oplysning om, hvem der er repræsentant for den dataansvarlige.[339] I den situation, hvor en myndighed indhenter oplysninger på vegne af en anden myndighed, f.eks. i den situation, hvor politiet

[336] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 28.
[337] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.1.1.
[338] Persondataloven med kommentarer (2015), s. 469.
[339] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 28.

indhenter oplysninger på vegne af Statsforvaltningen som led i behandlingen af en sag om samvær, skal der gives oplysning om, at det er Statsforvaltningen og ikke politiet, der er den dataansvarlige.[340]

Det følger af persondatalovens § 28, stk. 1, nr. 2, at der skal gives meddelelse om formålene med den behandling, hvortil oplysninger er bestemt. En identisk bestemmelse følger af databeskyttelsesdirektivets artikel 10, litra b.

Det følger af bemærkningerne til persondataloven, at der skal gives den registrerede tilstrækkelig information til, at den pågældende bliver klar over, hvad der er baggrunden for, at der indsamles oplysninger om den pågældende.[341] Kravet om formålsangivelse skal ses i sammenhæng med udtrykkelighedskravet i persondatalovens § 5, stk. 2. For en nærmere behandling af persondatalovens § 5, stk. 2, henvises der til afsnit 3.1. om principper for behandling af personoplysninger, hvoraf det bl.a. derudover fremgår, at der ved indsamlingen af oplysninger skal angives et formål, som er tilstrækkeligt veldefineret og velafgrænset til at skabe åbenhed og klarhed omkring behandlingen.

Det følger af Datatilsynets vejledning og af persondataloven med kommentarer, at de krav, der skal stilles til formålsangivelsen vil bero på en vurdering af de konkrete omstændigheder omkring behandlingen af oplysningerne. Da hensigten med bestemmelsen er at skabe åbenhed, må det dog som minimum kræves, at den registrerede underrettes om, hvad de indsamlede oplysninger skal bruges til eller påtænkes brugt til på indsamlingstidspunktet. Indsamlede oplysninger kan herefter i den periode, som er nødvendig hertil, behandles i disse øjemed. Oplysninger vil endvidere *i almindelighed* kunne behandles (benyttes) til andre efterfølgende saglige formål, uden at den dataansvarlige på ny skal give den registrerede meddelelse, hvis behandlingen ikke er uforenelig med det eller de formål, som oprindeligt er oplyst til den registrerede i forbindelse med opfyldelse af oplysningspligten. Kun *i særlige tilfælde* vil der påhvile den dataansvarlige en pligt til efterfølgende at oplyse om (nye) behandlingsformål, som ikke er omfattet af den oprindelige meddelelse, og som aktualiseres efter tidspunktet for indsamlingen af oplysninger.[342]

Fra praksis kan nævnes en sag, der bl.a. vedrørte spørgsmålet om oplysningspligt i en personalesag. I sagen var der udarbejdet fem notater på baggrund af fem samtaler med en ansat om dennes arbejde, der efterfølgende blev anvendt i forbindelse med afskedigelse af den ansatte. Det var Datatilsynets vurdering, at formålet med at indhente den ansattes til-

[340] Persondataloven med kommentarer (2015), s. 470.
[341] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 28.
[342] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.1.3 og Persondataloven med kommentarer (2015), s. 470.

kendegivelser og vurderinger havde været klart i de konkrete samtalesituationer. På denne baggrund var det Datatilsynets opfattelse, at inddragelsen – og dermed den efterfølgende brug – af de omhandlede oplysninger i afskedigelsen ikke udløste krav om ny meddelelse efter persondatalovens § 28. Der blev herved lagt vægt på, at det måtte have stået klart for den ansatte, at der foregik en bedømmelse og evaluering af den pågældendes arbejde og adfærd, og at forløbet af de stedfundne samtaler ville indgå heri.[343]

Derudover kan der fra Datatilsynets praksis nævnes en sag, der vedrørte behandling af personoplysninger hos Center for Seksuelt Misbrugte Øst (CSMØ). Her udtalte Datatilsynet, at de følsomme oplysninger, som CSMØ indsamlede og registrerede – under hensyntagen til karakteren af oplysningerne og til *det ganske særlige formål*, der begrundede behandlingen – ikke uden samtykke kunne videregives eller behandles til andre formål end de, der blev varetaget af centret. Dette gjaldt dog ikke i de tilfælde, hvor pligtmæssig videregivelse fulgte af lov.[344]

Fra Datatilsynets praksis kan også nævnes en sag, der bl.a. vedrørte spørgsmålet om, hvorvidt videregivelse af oplysninger til brug for vurderinger af personers kreditværdighed medførte en ny oplysningspligt efter persondatalovens § 21, jf. persondatalovens §§ 28-29. Et kreditoplysningsbureau havde indsamlet oplysninger om en række registrerede og havde i den forbindelse udsendt en registreringsmeddelelse, hvoraf det fremgik, at registreringen på et senere tidspunkt ville kunne blive videregivet til alle bureauets kunder. Det fremgik ikke af meddelelsen, at registreringen ville kunne blive anvendt ved udformning af bredere bedømmelser. I den forbindelse udtalte Datatilsynet, at de i sagen indsamlede oplysninger i almindelighed endvidere ville kunne behandles (benyttes) til andre efterfølgende saglige formål, uden at den dataansvarlige på ny skulle give den registrerede meddelelse, hvis behandlingen ikke var uforenelig med det eller de formål, som oprindeligt var oplyst til den registrerede i forbindelse med opfyldelsen af oplysningspligten. Datatilsynet udtalte derudover, at der kun i særlige tilfælde ville påhvile den dataansvarlige en pligt til efterfølgende at oplyse om (nye) behandlingsformål, som ikke var omfattet af den oprindelige meddelelse, og som blev aktualiseret efter tidspunktet for indsamlingen af oplysninger. Datatilsynet udtalte derudover, at anvendelsen af de lukkede registreringer til bredere bedømmelser ikke kunne anses for uforeneligt med de formål, hvortil oplysninger var registreret. Endelig udtalte Datatilsynet, at det endvidere var tilsynets opfattelse, at anvendelse af RKI's lukkede registreringer til beregning af Consumer Delphi score og Commercial Delphi score ikke

[343] Sag vedrørende spørgsmål om oplysningspligt og indsigtsret i personalesag, Datatilsynets j.nr. 2010-313-0384.
[344] Sag vedrørende behandling af personoplysninger hos Center for Seksuelt Misbrugte Øst, Datatilsynets j.nr. 2013-42-0962.

medførte krav om ny registreringsmeddelelse til de personer og/eller virksomheder, der allerede var registreret med en betalingsanmærkning hos selskabet.[345]

Derudover skal der i medfør af persondatalovens § 28, stk. 1, nr. 3, der er baseret på databeskyttelsesdirektivets artikel 10, litra c, gives en række yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysninger er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser. § 28 nævner i litra a–c, at sådanne yderligere oplysninger f.eks. kan være kategorierne af modtagere, om det er obligatorisk eller frivilligt at besvare stillede spørgsmål samt mulige følger af ikke at svare og om reglerne i indsigt i og berigtigelse af de oplysninger, der vedrører den registrerede.

Det følger af bemærkningerne til persondataloven, at det skal afgøres konkret i det enkelte tilfælde om og i givet fald, hvilke yderligere oplysninger der skal gives, og at oplistning i litra a–c ikke er udtømmende, hvorfor der kan påhvile den dataansvarlige en pligt til at give den registrerede andre oplysninger. Særligt kan der – efter omstændighederne – påhvile den dataansvarlige en pligt til at oplyse den registrerede om reglerne om sletning.

Oplysningspligten omfatter som udgangspunkt alene oplysninger, som på indsamlingstidspunktet må anses for nødvendige i bestemmelsens forstand. Efter omstændighederne kan der dog påhvile den dataansvarlige en pligt til også at oplyse om (nye) forhold, som ikke er omfattet af den oprindelige meddelelse, og som først aktualiseres efter tidspunktet for indsamlingen af oplysningerne.[346]

I forhold til litra a om *kategorierne af modtagere* følger det af Datatilsynets vejledning, at der ikke skal gives den registrerede ny meddelelse, hver gang indsamlede oplysninger meddeles til en ny modtager, der falder ind under de kategorier af modtagere, som oprindeligt er oplyst til den registrerede. Begrebet modtager er defineret i persondataloven § 3, stk. 7, hvoraf det fremgår, at myndighederne, der vil kunne få tildelt oplysninger som led i en isoleret forespørgsel, ikke betragtes som modtagere. Derudover vil anvendelsen af oplysningerne i forskellige afdelinger og lignende inden for samme myndighed ikke betragtes som en overførsel til en ny modtager.[347] Omvendt vil f.eks. en videregivelse fra et departement til en underliggende styrelse betragtes som en overførsel til en ny modtager. På samme måde vil en videregivelse fra et moderselskab til et datterselskab ligeledes betragtes som en overførsel til en ny modtager.

[345] Sag om Consumer Delphi og Commercial Delphi, Datatilsynets j. nr. 2005-631-0161.
[346] Persondataloven med kommentarer (2015), s. 471.
[347] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.1.3.

I sag C-201/14, Bara, dom af 1. oktober 2015, havde en offentlig myndighed videregivet personoplysninger til en anden offentlig myndighed, der havde foretaget behandling af disse personoplysninger, uden at nogen af myndighederne havde oplyst de registrerede om videregivelse eller behandling.

EU-Domstolen udtalte i præmis 34, at kravet om rimelig behandling i databeskyttelsesdirektivets artikel 6 forpligter en offentlig myndighed til at underrette de registrerede om videregivelsen af oplysninger til en anden offentlig myndighed med henblik på disses behandling hos myndigheden i dennes egenskab af modtager af de nævnte oplysninger.

I en sådan situation, hvor de indsamlede oplysninger meddeles til en ny modtager, påhviler det samtidig denne nye modtager at vurdere, om den registrerede derudover skal underrettes efter databeskyttelsesdirektivets artikel 11, som er implementeret ved persondatalovens § 29, eller om det ikke er nødvendigt, fordi en af undtagelserne i persondatalovens § 29, stk. 2, finder anvendelse.

I forhold til litra b, *om det er obligatorisk eller frivilligt at besvare stillede spørgsmål samt mulige følger af ikke at svare*, følger det af Datatilsynets vejledning, at det må anses som et naturligt led i forbindelse med indsamlingen, at den dataansvarlige informerer den registrerede om eventuelt strafansvar for ikke at besvare en henvendelse om at få oplysningerne eller på anden måde give indberetning.[348]

I forhold til litra c, *om reglerne i indsigt i og berigtigelse af de oplysninger, der vedrører den registrerede,* antages det, at hvis den registrerede retter uopfordret henvendelse til den dataansvarlige med oplysninger om sig selv, vil der i almindelighed ikke være behov for at oplyse herom. Hvis indsamlingen af oplysninger sker gennem en blanket, et ansøgningsskema eller lignende, vil den dataansvarlige dog uden større udgift kunne give oplysningerne gennem en fortrykt, generel vejledning på blanketten mv.[349]

Meget taler for, at en dataansvarlig, der indsamler oplysninger hos en registreret person, skal underrette den pågældende om, at oplysningerne vil blive gjort til genstand for en automatiseret afgørelse, og at den pågældende i den forbindelse har indsigelsesret mv. efter persondatalovens § 39.[350]

[348] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.1.3.
[349] Persondataloven med kommentarer (2015), s. 472.
[350] Persondataloven med kommentarer (2015), s. 472.

4.3.2.2. Persondatalovens § 28, stk. 2

Det fremgår af persondatalovens § 28, stk. 2, der er baseret på databeskyttelsesdirektivets artikel 10, at bestemmelsen i stk. 1 ikke gælder, hvis den registrerede allerede er bekendt med de i nr. 1–3 nævnte oplysninger.

Det følger af Datatilsynets vejledning, at denne undtagelsesbestemmelse navnlig har dens baggrund i, at en ubetinget oplysningspligt ville være for vidtgående i forhold til den dataansvarlige, der ville blive påført betydelige omkostninger, som ikke i alle tilfælde ville stå mål med det udbytte, en registreret person har af at modtage underretning om, at der indsamles oplysninger om vedkommende.[351]

Det vil bero på en konkret vurdering, om den registrerede allerede er bekendt med oplysningerne. I de situationer, hvor indsamlingen af oplysninger sker ved, at den registrerede selv har rettet henvendelse til den dataansvarlige, vil det almindeligvis kunne lægges til grund, at den registrerede allerede er bekendt med de oplysninger, der efter persondatalovens § 28, stk. 1, skal gives den pågældende. Den registrerede vil som altovervejende hovedregel være bekendt med den *dataansvarliges identitet* samt *formålene* med den behandling, hvortil oplysningerne er bestemt. I de situationer, hvor den dataansvarlige aktivt indsamler oplysninger hos den registrerede (f.eks. gennem en ansøgningsblanket), vil det i mange tilfælde kunne lægges til grund, at den registrerede allerede er bekendt med de i persondatalovens § 28 stk. 1, nr. 1 og 2, anførte oplysninger.[352] Derudover vil det i almindelighed ikke være nødvendigt at give den registrerede *yderligere oplysninger,* i medfør af persondatalovens § 28, stk. 1, nr. 3, for at den pågældende kan varetage sine interesser.[353]

Det følger dog af bemærkningerne til persondataloven, at hvis den dataansvarlige eller dennes repræsentant er i tvivl om, hvorvidt den registrerede allerede er bekendt med oplysningerne, så skal der gives meddelelse i overensstemmelse med stk. 1.[354]

Fra praksis kan nævnes en sag vedrørende en myndigheds offentliggørelse af oplysninger om en borger i et udvalgs beslutningsprotokol på en kommunes hjemmeside. Her var det Datatilsynets opfattelse, at en sådan offentliggørelse må anses for et almindeligt sagsbehandlingsskridt på linje med journalisering. Der var således efter Datatilsynets opfattelse ikke tale om, at oplysningerne om borgeren anvendes til et andet formål end til behandling

[351] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.3.
[352] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.3.1.1.
[353] Persondataloven med kommentarer (2015), s. 473.
[354] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 28.

af sagen. På den baggrund var det Datatilsynets vurdering, at offentliggørelse af oplysninger om borgeren i Økonomiudvalgets beslutningsprotokol på kommunens hjemmeside ikke medførte krav om en selvstændig og individuel meddelelse i medfør af persondatalovens §§ 28 og 29.[355]

4.3.3. Databeskyttelsesforordningen

Databeskyttelsesforordningen fastsætter en pligt til at give den registrerede en række oplysninger ved indsamling af personoplysninger hos den registrerede, jf. artikel 13, stk. 1 og 2. Den dataansvarlige skal i øvrigt i medfør af forordningens artikel 30, stk. 1, føre en fortegnelse over behandlingsaktiviteter, der skal indeholde en række af de oplysninger, som den dataansvarlige skal give den registrerede i medfør af forordningens artikel 13, stk. 1 og 2.

4.3.3.1. Databeskyttelsesforordningens artikel 13, stk. 1

Det fremgår af forordningens artikel 13, stk. 1, at den dataansvarlige, ved indsamling af personoplysninger hos den registrerede, på tidspunktet for denne indsamling skal give den registrerede de oplysninger, der følger af bestemmelsens litra a–f. Oplistningen i bestemmelsen er udtømmende.

4.3.3.1.1. Databeskyttelsesforordningens artikel 13, stk. 1, litra a

Det fremgår af forordningens artikel 13, stk. 1, litra a, at den dataansvarlige skal give oplysning om identitet på og kontaktoplysninger for den dataansvarlige og dennes eventuelle repræsentant.

Dette krav følger allerede af persondatalovens § 28, stk. 1, nr. 1. Det er dog nyt, at der også altid skal gives kontaktoplysninger, hvorved der antageligvis menes telefonnummer, e-mailadresse eller lignende.

4.3.3.1.2. Databeskyttelsesforordningens artikel 13, stk. 1, litra b

Det fremgår af forordningens artikel 13, stk. 1, litra b, at den dataansvarlige skal give oplysning om kontaktoplysninger for en eventuel databeskyttelsesrådgiver. For en nærmere gennemgang af, hvem der skal udpege en databeskyttelsesrådgiver i medfør af forordningens artikel 37, henvises til afsnit 5.17. og 5.18.

Da rollen som databeskyttelsesrådgiver er ny i medfør af forordningen, vil det således også være nyt, at der skal gives kontaktoplysninger for en eventuel databeskyttelsesrådgiver.

[355] Sag vedrørende offentliggørelse af navn og adresse på kommunes hjemmeside, Datatilsynets j.nr. 2004-313-0247.

4.3.3.1.3. Databeskyttelsesforordningens artikel 13, stk. 1, litra c
Det fremgår af forordningens artikel 13, stk. 1, litra c, at den dataansvarlige skal give oplysning om formålene med og retsgrundlaget for behandlingen.

Det følger allerede af persondatalovens § 28, stk. 1, nr. 2, at der altid skal gives den registrerede meddelelse om formålene med den behandling, som personoplysningerne skal bruges til.

Derimod er det nyt, at der altid skal gives oplysninger om retsgrundlaget for behandlingen.

Det fremgår bl.a. af præambelbetragtning nr. 41, at når der i forordningen henvises til retsgrundlag, kræver det ikke nødvendigvis en lov, der er vedtaget af et parlament. Retsgrundlaget kan således også udgøres af en bekendtgørelse.

Det fremgår endvidere af præambelbetragtning nr. 45, at denne forordning ikke indebærer, at der kræves en specifik lov til hver enkelt behandling. Det kan være tilstrækkeligt med en lov som grundlag for adskillige databehandlingsaktiviteter, som baseres på en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse.

Formålet med bestemmelsen i artikel 13, stk. 1, litra c, er at sikre, at den registrerede kan varetage sine interesser. Når den dataansvarlige skal oplyse om retsgrundlaget for behandlingen, skal der henvises til den lov eller bekendtgørelse, hvor det følger, at oplysningerne må indsamles. Dette kan f.eks. ske ved at henvise til, at indsamling sker efter den sociale retssikkerhedslovs bestemmelser. Den dataansvarlige kan ikke alene henvise generelt til f.eks., at det sker som led i udførelse af en opgave i samfundets interesse eller, at det henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Der må således skulle henvises til det konkrete retsgrundlag, eventuelt det relevante kapitel i en lov eller bekendtgørelse. I det tilfælde, at behandling af personoplysninger alene sker med hjemmel i forordningens behandlingsbestemmelser, vil der skulle henvises til den relevante bestemmelse i forordningen.

At den dataansvarlige efter forordningen altid skal give meddelelse om retsgrundlaget for behandlingen er nyt i forhold til gældende ret. Den dataansvarlige skal dog allerede, når der foretages en vurdering af, om der må foretages behandling af personoplysninger, vurdere hjemmelsgrundlaget for behandling i medfør af persondatalovens behandlingsregler eller regler i særlovgivningen. Meddelelsen af retsgrundlaget for behandlingen må kunne ske ved, at den dataansvarlige f.eks. indsætter et yderligere afsnit i et ansøgningsskema eller lignende.

4.3.3.1.4. Databeskyttelsesforordningens artikel 13, stk. 1, litra d
Det fremgår af forordningens artikel 13, stk. 1, litra d, at den dataansvarlige skal give oplysning om de legitime interesser, som forfølges af den dataansvarlige eller en tredjemand, *hvis* behandlingen er baseret på artikel 6, stk. 1, litra f.

Det bemærkes, at artikel 6, stk. 1, litra f, ikke gælder for behandling af personoplysninger, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

Det er nyt i forhold til gældende ret, at der altid skal oplyses om de legitime interesser, der forfølges. Den dataansvarlige skal dog allerede i dag foretage en vurdering af de legitime interesser, jf. databeskyttelsesdirektivets artikel 7, litra f, og persondatalovens § 6, stk. 1, nr. 7.

4.3.3.1.5. Databeskyttelsesforordningens artikel 13, stk. 1, litra e
Det fremgår af forordningens artikel 13, stk. 1, litra e, at den dataansvarlige skal give oplysning om eventuelle modtagere eller kategorier af modtagere.

Det følger af gældende ret, at der skal foretages en vurdering af, om det i det konkrete tilfælde vil være nødvendigt at meddele om modtagerne *eller* kategorierne af modtagere for at sikre den registrerede en rimelig behandling af oplysningerne, jf. databeskyttelsesdirektivets artikel 10, stk. 1, nr. 3, og persondatalovens § 28, stk. 1, nr. 3, litra a. Dog følger det, at såfremt det på tidspunktet for indsamlingen af oplysninger må stå den dataansvarlige klart, at oplysningerne skal videregives til andre modtagere, skal den dataansvarlige allerede efter gældende ret oplyse den registrerede om kategorierne af modtagere.

Med betegnelsen "kategorierne af modtagere" i direktivet og i forordningen må der – bl.a. i lyset af de gældende krav til oplysningspligt – alene antages at være tale om overordnede angivelser af modtagere såsom "andre offentlige myndigheder", "samarbejdspartnere", "datterselskaber" mv.

Forordningen tager ved ordet "*eventuelle*" forbehold for, at det ikke altid er tiltænkt, at der skal være andre modtagere af oplysningerne end den dataansvarlige. Det må forstås sådan, at den dataansvarlige ikke er forpligtet til at give oplysning om dette forhold til den registrerede, hvis der ikke på tidspunktet for indsamlingen er andre modtagere end den dataansvarlige. Det vil således ikke være nødvendigt f.eks. at skrive, at de indsamlede oplysningerne ikke påtænkes videregivet til andre modtagere eller kategorier af modtagere.

4.3.3.1.6. Databeskyttelsesforordningens artikel 13, stk. 1, litra f

Det fremgår af forordningens artikel 13, stk. 1, litra f, at den dataansvarlige, hvor det er relevant, skal give meddelelse om, at den dataansvarlige agter at overføre personoplysninger til et tredjeland eller en international organisation, og om hvorvidt Kommissionen har truffet afgørelse om tilstrækkeligheden af beskyttelsesniveauet, eller i tilfælde af overførsler i henhold til artikel 46 eller 47 eller artikel 49, stk. 1, 2. afsnit, henvisning til de fornødne eller passende garantier, og hvordan der kan fås en kopi heraf, eller hvor de er blevet gjort tilgængelige.

Det følger af formuleringen, "*hvor det er relevant"*, at den dataansvarlige ikke skal give oplysning, såfremt den dataansvarlige ikke agter at overføre personoplysninger på de måder, som bestemmelsen oplister.

Oplysning om overførsel til tredjelande vil efter omstændighederne være en del af de yderligere oplysninger, der følger af persondatalovens § 28, stk. 1, nr. 3. I medfør af denne er der alene pligt til at oplyse om overførsler til tredjelande, såfremt det – på baggrund af en konkret vurdering – er nødvendigt for, at den registrerede kan varetage sine interesser. Ved denne vurdering skal der tages hensyn til de særlige omstændigheder, hvorunder oplysninger er indsamlet. Forordningen ændrer på gældende ret ved altid at gøre det til en betingelse at oplyse herom, hvis den dataansvarlige agter at overføre personoplysninger til tredjelande eller internationale organisationer.

4.3.3.2. Databeskyttelsesforordningens artikel 13, stk. 2

Det følger af forordningens artikel 13, stk. 2, at den dataansvarlige skal give den registrerede – på det tidspunkt, hvor personoplysningerne indsamles – en række yderligere oplysninger, der er nødvendige for at sikre en rimelig og gennemsigtig behandling. Disse yderligere oplysninger er fastsat i litra a–f. Opdelingen i forordningen af artikel 13 i en stk. 1, med oplysninger, der altid *skal* meddeles den registrerede, og en stk. 2, med oplysninger, der er *nødvendige for at sikre en rimelig og gennemsigtig behandling*, må betyde, at den dataansvarlige i medfør af stk. 2, skal foretage en konkret vurdering af, om der skal gives den registrerede yderligere oplysninger, end hvad der allerede kræves i medfør af artikel 13, stk. 1.

Denne forståelse stemmer overens med præambelbetragtning nr. 60, hvoraf det følger, at den dataansvarlige bør give den registrerede *eventuelle yderligere oplysninger*, der er nødvendige for at sikre en rimelig og gennemsigtig behandling, under hensyntagen til de specifikke omstændigheder og forhold, som personoplysningerne behandles under. Derudover følger det af betragtningen, at hvis personoplysninger indsamles fra den registrerede, bør den registrerede informeres om, hvorvidt den pågældende er forpligtet til at meddele per-

sonoplysninger og om konsekvenserne af ikke at meddele. Denne information *kan* gives sammen med standardiserede ikoner med henblik på at give et meningsfuldt overblik over den planlagte behandling på en klart synlig, letlæselig og letforståelig måde. Hvis ikonerne præsenteres elektronisk, bør de være maskinlæsbare.

4.3.3.2.1. Databeskyttelsesforordningens artikel 13, stk. 2, litra a
Det fremgår af forordningens artikel 13, stk. 2, litra a, at den dataansvarlige skal give oplysninger om det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum.

Denne pligt afspejler kravet om, at en dataansvarlig ikke må opbevare indsamlede oplysninger på en måde, der giver mulighed for at identificere den registrerede i længere tidsrum, end det er nødvendigt af hensyn til de formål, hvortil oplysninger indsamles, jf. forordningens artikel 5, stk. 1, litra e.

Den dataansvarlige skal i medfør af gældende ret foretage en vurdering af, hvor længe indsamlede oplysninger skal opbevares, og til hvilket formål de opbevares.

Det følger af forordningens artikel 30, stk. 1, litra f, om fortegnelser af behandlingsaktiviteter, at sådanne, hvis det er muligt, skal indeholde de forventede tidsfrister for sletning af forskellige kategorier af oplysninger.

Såfremt det ikke på tidspunktet for indsamlingen er muligt at vurdere, hvor længe oplysninger vil blive opbevaret, giver forordningen mulighed for at beskrive de kriterier, der anvendes til at fastlægge dette tidsrum. I og med der er tale om et alternativ til at fastsætte en konkret opbevaringsperiode, må der navnlig tænkes på momenter, som kan være med til at forlænge/forkorte opbevaringsperioden.

Det følger allerede af gældende ret, at en dataansvarlig skal vurdere, hvor længe oplysninger om den registrerede opbevares. Det er imidlertid en ny betingelse, at den registrerede på tidspunktet for indsamlingen af oplysninger skal oplyses om enten dette tidsrum eller de kriterier, der anvendes til at fastlægge dette tidsrum. Som eksempel på hvad der må antages at udgøre en passende oplysning om de kriterier, der anvendes til at fastlægge tidsrummet, kan den dataansvarlige f.eks. oplyse, at oplysninger gemmes i lyset af de relevante regler om forældelse af formueretlige krav.

4.3.3.2.2. Databeskyttelsesforordningens artikel 13, stk. 2, litra b
Det fremgår af forordningens artikel 13, stk. 2, litra b, at den dataansvarlige skal oplyse om retten til at anmode om indsigt i og berigtigelse eller sletning af personoplysninger eller

begrænsning af behandling vedrørende den registrerede eller til at gøre indsigelse mod behandling samt retten til dataportabilitet.

Derudover fremgår det af forordningens artikel 21, stk. 4, at den dataansvarlige specifikt vedrørende retten til indsigelse mod behandling baseret på enten artikel 6, stk. 1, litra e og f, eller på direkte markedsføring senest på tidspunktet for den første kommunikation med den registrerede udtrykkeligt skal gøre den registrerede opmærksom på retten til indsigelse efter artikel 21, stk. 1 og 2. Meddelelse herom skal være klar og adskilt fra alle andre oplysninger.

For en nærmere behandling henvises til afsnit 4.11. om ret til indsigelse.

Det følger af gældende ret, at den dataansvarlige skal foretage en vurdering af, om det er nødvendigt for den registrerede, for at denne kan varetage sine interesser, at der gives oplysning om reglerne om indsigt i og om berigtigelse af oplysninger, der vedrører den registrerede, jf. persondatalovens § 28, stk. 1, nr. 3, litra c. Som det følger ovenfor, skal den registrerede efter omstændighederne også oplyses om reglerne om sletning.

For så vidt angår retten til begrænsning af behandling af den registrerede og retten til dataportabilitet findes tilsvarende bestemmelser ikke i gældende ret, hvorfor den dataansvarlige i medfør af forordningen også bør vurdere, om der skal oplyses om de nævnte forhold.

4.3.3.2.3. Databeskyttelsesforordningens artikel 13, stk. 2, litra c

Det fremgår af forordningens artikel 13, stk. 2, litra c, at den dataansvarlige, når behandling er baseret på artikel 6, stk. 1, litra a, eller artikel 9, stk. 2, litra a, skal oplyse om retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf.

Det bemærkes, at dette også er en betingelse for et gyldigt samtykke efter forordningens artikel 7, stk.3.

Der findes ikke en tilsvarende bestemmelse i gældende ret, der specifikt forpligter den dataansvarlige til at vurdere, hvorvidt den registrerede skal oplyses om retten til at tilbagekalde et samtykke. Dette nye krav vil enkelt kunne iagttages ved at indsætte et afsnit i ansøgningsskemaer mv. Derudover følger det af forordningens artikel 12, stk. 7, at der sammen med iagttagelsen af oplysningspligten *kan* gives standardiserede ikoner, hvorfor der antageligvis også foreligger en mulighed for gennem et sådant ikon at linke til oplysninger om retten til at tilbagetrække et samtykke. For en nærmere behandling henvises der til afsnit 4.1. om artikel 12.

4.3.3.2.4. Databeskyttelsesforordningens artikel 13, stk. 2, litra d
Det fremgår af forordningens artikel 13, stk. 2, litra d, at den dataansvarlige skal oplyse om retten til at indgive en klage til en tilsynsmyndighed.

Det følger ikke af gældende ret, at der skal gives oplysning om retten til at indgive klage i forbindelse med indsamling af oplysninger. I og med, at der er tale om indgivelse af klage til den nationale tilsynsmyndighed, vil denne nye forpligtelse kunne opfyldes ved at indsætte et standardiseret afsnit i ansøgningsskemaer og lignende, hvoraf retten til at indgive klage fremgår.

4.3.3.2.5. Databeskyttelsesforordningens artikel 13, stk. 2, litra e
Det fremgår af forordningens artikel 13, stk. 2, litra e, at der skal gives oplysning om meddelelse af personoplysninger er lovpligtigt eller et krav i henhold til en kontrakt eller et krav, der skal være opfyldt for at indgå en kontrakt, samt om den registrerede har pligt til at give personoplysninger og de eventuelle konsekvenser af ikke at give sådanne oplysninger.

Det følger af gældende ret, at der efter omstændighederne skal gives meddelelse om, hvorvidt det er obligatorisk eller frivilligt at besvare stillede spørgsmål samt mulige følger af ikke at svare, jf. persondatalovens § 28, stk. 1, nr. 3, litra b, og direktivets artikel 10, litra c. Den ændrede ordlyd medfører ikke ændringer af den gældende retstilstand, hvilket stemmer overens med, at bestemmelsen var en del af Kommissionens oprindelige forordningsforslag, og at Kommissionen ikke mener, at betingelsen tilføjer noget nyt i forhold til databeskyttelsesdirektivet.[356]

Derudover synes der ikke i denne kontekst at være en sproglig forskel på *eventuelle konsekvenser* og *mulige følger*.

For så vidt angår oplysning om meddelelse af personoplysninger er lovpligtigt eller et krav i henhold til en kontrakt eller et krav, der skal være opfyldt for at indgå en kontrakt, ses samme specificering ikke i gældende ret. Der er derved tale om et nyt krav.

4.3.3.2.6. Databeskyttelsesforordningens artikel 13, stk. 2, litra f
Det fremgår af forordningens artikel 13, stk. 2, litra f, at der skal oplyses om forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og i disse tilfælde som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede.

[356] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), s. 9 og 51.

Det følger af formuleringen, *"forekomsten af"* at den dataansvarlige alene kan være underlagt en oplysningspligt, hvis automatiske afgørelser forekommer, hvorfor det ikke er nødvendigt at oplyse herom, når automatiske afgørelser ikke forekommer.

Når de dataansvarlige alene skal oplyse om "logikken" i automatiske afgørelser, kan det ikke kræves, at der gives en meget detaljeret beskrivelse af behandlingens grundlag. Det afgørende må være, at man som registreret kan forstå de overvejelser, der ligger til grund for behandlingen, og hvordan "systemet" kommer frem til de forskellige afgørelser.

I det omfang der er tale om en forvaltningsretlig afgørelse, supplerer artikel 13, stk. 2, litra f, her de forvaltningsretlige krav til begrundelse mv.

Denne bestemmelse vil f.eks. være relevant for virksomheder der, som et led i direkte markedsføring, indsamler personoplysninger til brug for at skabe en profil af en forbruger (profilering) som omhandlet i artikel 22. Her vil der være tale om en automatisk afgørelse, hvor det pålægges virksomheden, som dataansvarlig, også at oplyse forbrugeren om indholdet af forordningens artikel 13, stk. 2, litra f. Virksomheden skal samtidig opfylde de øvrige pligter i artikel 13. Bestemmelsen vil også være relevant for offentlige myndigheder, der benytter sig af automatiske afgørelser i sagsbehandlingen. Det bemærkes i den forbindelse, at en offentlig myndighed, der træffer en automatisk afgørelse f.eks. med hjemmel i en national lov i medfør af artikel 22, stk. 2, litra b, hvilket betyder, at artikel 22, stk. 1, ikke finder anvendelse, stadig skal overholde oplysningspligten i artikel 13, stk. 2, litra f.

Det er nyt i forordningen, at det direkte fremgår af bestemmelsen, at der påhviler den dataansvarlige en pligt til altid at foretage en konkret vurdering af, om der skal oplyses om forekomsten af automatiske afgørelser.

4.3.3.3. Databeskyttelsesforordningens artikel 13, stk. 3

Det følger af forordningens artikel 13, stk. 3, at hvis den dataansvarlige agter at viderebehandle personoplysningerne til *et andet formål* end det, hvortil de er indsamlet, giver den dataansvarlige forud for denne viderebehandling den registrerede oplysninger om dette andet formål og andre relevante yderligere oplysninger, jf. stk. 2.

Det følger af gældende ret, som gengivet ovenfor, at de krav, der skal stilles til formålsangivelsen vil bero på en vurdering af de konkrete omstændigheder omkring behandlingen af oplysningerne, og at oplysninger *i almindelighed* endvidere vil kunne behandles (benyttes) til andre, efterfølgende saglige formål, uden at den dataansvarlige på ny skal give den registrerede meddelelse, hvis behandlingen ikke er uforenelig med det eller de formål, som oprindeligt er oplyst til den registrerede i forbindelse med opfyldelse af oplysningspligten.

Det er kun *i særlige tilfælde*, at der vil påhvile den dataansvarlige en pligt til efterfølgende at oplyse om (nye) behandlingsformål, som ikke er omfattet af den oprindelige meddelelse, og som aktualiseres efter tidspunktet for indsamlingen af oplysninger.

Forordningen fastsætter, at der skal oplyses om, at den dataansvarlige agter at viderebehandle personoplysninger, når dette sker til et *andet formål*. Efter en ordlydsfortolkning, må denne ændring efter omstændighederne udvide området for, hvornår der skal gives en registreret meddelelse om viderebehandling af den pågældendes personoplysninger, i og med, at det efter forordningen vil være den blotte omstændighed, at formålet er et andet, der udløser ny oplysningspligt. Efter gældende ret har den dataansvarlige allerede skulle foretage en vurdering af en viderebehandlings uforenelighed med de allerede oplyste formål. Denne vurdering skal stadig foretages i medfør af forordningen, hvor betydningen af den ændrede ordlyd efter omstændighederne bliver, at den dataansvarlige oftere vil skulle oplyse den registrerede, når der foretages viderebehandling.

For så vidt angår kravet om at oplyse den registrerede om *andre relevante yderligere oplysninger* må den dataansvarlige i forbindelse med en viderebehandling foretage en konkret vurdering af, om det er nødvendigt for at sikre en *rimelig* og *gennemsigtig* behandling, at der gives den registrerede en række yderligere oplysninger, der følger af artikel 13, stk. 2. Det er ved denne vurdering oplagt at overveje, om den registrerede allerede er bekendt med oplysningerne, hvorfor en meddelelse ikke er nødvendig, jf. artikel 13, stk. 4.

4.3.3.4. Databeskyttelsesforordningens artikel 13, stk. 4

Det følger af forordningens artikel 13, stk. 4, at hvis og i det omfang, at den registrerede allerede er bekendt med de oplysningerne, der skal meddeles i medfør af artikel 13, stk. 1–3, så finder artikel 13, stk. 1–3, ikke anvendelse, hvorfor der ikke gælder en oplysningspligt for den dataansvarlige.

Ordlyden af bestemmelsen i persondatalovens § 28, stk. 2, der baserer sig på databeskyttelsesdirektivets artikel 10, er i al væsentlighed identisk med artikel 13, stk. 4, hvorfor der allerede i dag gælder en undtagelse til oplysningspligten, såfremt den registrerede er bekendt med oplysningerne.

Forordningens artikel 13, stk. 1-3, udvider dog omfanget af de oplysninger, som den dataansvarlige skal meddele den registrerede. Denne udvidelse har betydning for anvendelsen af forordningens artikel 13, stk. 4, i praksis. Det vil i fremtiden således være sjældnere, at oplysningspligt helt kan undlades.

4.3.4. Overvejelser

Vedrørende databeskyttelsesforordningens artikel 13, stk. 1, følger det allerede af gældende ret, at der skal gives meddelelse om identitet på den dataansvarlige samt formålene med den behandling, der foretages. Derudover følger det også af gældende ret, at der skal foretages en vurdering af, om der efter omstændighederne skal gives oplysning om eventuelle modtagere eller kategorier af modtagere.

Forordningen udvider området for de oplysninger, der skal gives, når personoplysninger behandles om den registrerede ved at pålægge den dataansvarlige en pligt til at give meddelelse om kontaktoplysninger på en eventuel databeskyttelsesrådgiver, kontaktoplysninger for den dataansvarlige og dennes repræsentant, retsgrundlaget for behandlingen, de legitime interesser, der forfølges samt, hvis det er relevant, overførsler i medfør af forordningens artikel 45–47 og artikel 49.

Vedrørende databeskyttelsesforordningens artikel 13, stk. 2, følger det allerede af gældende ret, at den dataansvarlige skal foretage en vurdering af, om der efter omstændighederne skal oplyses om reglerne om indsigt i og berigtigelse samt sletning af oplysninger, om retten til at tilbagekalde et samtykke, om pligten til at give oplysninger samt om konsekvenser af ikke at svare.

Forordningen udvider området for de oplysninger, der, efter en konkret vurdering, skal meddeles den registrerede ved at specificere, at der skal foretages en vurdering af tidsperioden for opbevaring af oplysninger, retten til begrænsning af behandling af oplysninger, retten til dataportabiliet, retten til at indgive klage til en tilsynsmyndighed, hvorvidt personoplysninger skal meddeles af den registrerede som følge af lov eller kontrakt samt om forekomsten af automatiske afgørelser.

Forordningens artikel 13, stk. 3, udvider området for den dataansvarliges oplysningspligt over for den registrerede, ved at denne også gælder, når der foretages viderebehandling af personoplysninger til andre formål end det, hvortil personoplysningerne er indsamlet.

Derudover følger det af udvidelsen af den dataansvarliges oplysningspligt over for den registrerede, at den dataansvarlige sjældnere vil kunne undlade at oplyse med henvisning til, at den registrerede allerede er bekendt med oplysningerne med henvisning til forordningens artikel 13, stk. 4.

Dog skal det bemærkes, at standardiserede ikoner i medfør af artikel 12, stk. 7 og 8, kan anvendes af den dataansvarlige for at opfylde oplysningspligten i artikel 13 og 14.

Forordningen udvider med artikel 13 generelt omfanget af den dataansvarliges oplysningspligt. Den dataansvarlige skal dog allerede foretage en række vurderinger i forbindelse med behandling af oplysninger efter de generelle behandlingsregler i medfør af persondatalovens kapitel 4.

4.4. Oplysningspligt, hvis personoplysningerne ikke er indsamlet hos den registrerede, artikel 14

4.4.1. Præsentation

I persondatalovens § 29 er der fastsat en pligt til at oplyse den registrerede om en række forhold ved oplysninger, der ikke er indsamlet hos den registrerede.

Forordningens artikel 14 indeholder en tilsvarende oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede.

4.4.2. Gældende ret

4.4.2.1. Persondatalovens § 29, stk. 1

Det fremgår af persondatalovens § 29, stk. 1, nr. 1–3, at den dataansvarlige eller dennes repræsentant, når oplysninger ikke er indsamlet hos den registrerede, ved registrering eller ved videregivelse til tredjemand skal oplyse den registrerede om en række forhold. Denne bestemmelse er baseret på artikel 11 i databeskyttelsesdirektivet, der fastsætter en tilsvarende oplysningspligt ved oplysninger, der ikke er indsamlet hos den registrerede.

Det fremgår af præambelbetragtning nr. 38 i databeskyttelsesdirektivet, at en rimelig behandling forudsætter, at de registrerede kan få kendskab til en behandlings eksistens, og når der indsamles oplysninger hos dem, kan få nøjagtig og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen.

Dette har en nær sammenhæng med præambelbetragtning nr. 39, hvoraf det følger, at for oplysninger, som ikke er indsamlet direkte hos den registrerede, eller der videregives til tredjemand, skal den registrerede underrettes, når oplysninger registreres, eller senest når oplysningerne første gang videregives til tredjemand.

Persondatalovens § 30 fastsætter en række undtagelser til oplysningspligten i § 29.

Det følger af bemærkningerne til persondataloven, at den dataansvarlige eller dennes repræsentant af egen drift skal meddele den registrerede de omhandlede oplysninger. Det følger derudover, at oplysningspligten enten indtræder ved registreringen af de indsamlede

oplysninger, eller, hvis de indsamlede oplysninger er bestemt til videregivelse til tredjemand, senest når oplysningerne videregives. Det er alene i de tilfælde, hvor indsamlede oplysninger er bestemt til videregivelse til tredjemand, at oplysningspligten skubbes, hvorfor det på tidspunktet for indsamlingen må være klart, om oplysningerne skal videregives til tredjemand. Endelig skal videregivelsen til tredjemand ske inden for en forholdsvis snæver periode.[357]

Datatilsynet har i en udtalelse slået fast, at en *indsamling af oplysninger* om en ansat fra dennes kolleger må anses for at være omfattet af persondatalovens § 29. I den konkrete sag havde en kommune indsamlet oplysninger om en ansat fra dennes kolleger som led i en prøvetidsevaluering. I og med, at denne indsamling af oplysninger ikke var sket hos den registrerede, var situationen omfattet af persondatalovens § 29.[358] I andre sammenhænge, hvor de ansatte udveksler personoplysninger som led i varetagelsen af deres opgaver, må der derimod være tale om en intern udveksling, som ikke medfører oplysningspligt efter persondatalovens § 29.[359]

Det fremgår ikke af loven eller dens forarbejder, hvad der skal forstås ved udtrykket "ved registrering". Under hensyntagen til, at udtrykket skal fastlægges på baggrund af databeskyttelsesdirektivets artikel 11, stk. 1, må det formentlig forstås som dækkende over den omstændighed, at personoplysninger undergives edb-behandling (automatisk behandling) eller indføres i et manuelt register.[360]

Det følger af Datatilsynets vejledning, at den tidsfrist, der kan indlægges i begrebet "ved registreringen" afhænger af sagens nærmere omstændigheder. Den dataansvarlige skal dog altid - vurderet i forhold til den indsats, der kræves fra den dataansvarliges side for at opfylde oplysningspligten - give den registrerede meddelelse så tidligt som muligt. Oplysningspligten vil i almindelighed skulle opfyldes inden for 10 dage efter registreringen. Hvis den dataansvarlige allerede på selve registreringstidspunktet ved, at der i løbet af ganske kort tid herefter skal rettes henvendelse til den registrerede, f.eks. fordi den dataansvarlige skal forelægge sagens dokumenter for den registrerede, eller der skal foretages andre sagsbehandlingsskridt, vil oplysningspligten som altovervejende hovedregel kunne opfyl-

[357] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 29.
[358] Udtalelse om opfyldelse af oplysningspligt ved indsamling af oplysninger hos kolleger, Datatilsynets j. nr.: 2007-313-0049.
[359] Persondataloven med kommentarer (2015), s. 476.
[360] Persondataloven med kommentarer (2015), s. 476.

des samtidig med denne senere henvendelse.[361] Af den grund må den dataansvarlige ikke opfylde oplysningspligten senere end dennes første henvendelse til den registrerede.

Datatilsynet har udtalt sig om den tidsmæssige udstrækning af oplysningspligten i en konkret sag, der omhandlede et forsikringsselskabs behandling af personoplysninger om klager og hendes børn i forbindelse med videooptagelser og observationer som led i forsikringsselskabets behandling af erstatningskrav rejst af klager over for forsikringsselskabet. Forsikringsselskabet havde overvåget klager, uden hendes vidende, i november og december 2009, og gjorde først klager opmærksom på denne overvågning i april 2010, hvor forsikringsselskabet sendte en fax til Arbejdsskadestyrelsen og klagers advokat om, at selskabet havde overvåget klager. Det var Datatilsynets opfattelse, at forsikringsselskabet ikke havde fremført vægtige argumenter for, at private interesser ville lide skade af væsentlig betydning, hvis underretningspligten blev opfyldt umiddelbart efter afslutningen af overvågningen. Datatilsynet fandt på den baggrund, at det var beklageligt, at der gik ca. 4 måneder, før klager blev underrettet om overvågningen, idet dette tidsrum ikke kunne karakteriseres som "inden for ganske kort tid", jf. pkt. 2.2.1. i rettighedsvejledningen.[362]

Derudover ses kravene i persondatalovens § 29, stk. 1, nr. 1 og 2, f.eks. for så vidt angår formkrav og om, at den dataansvarlige alene er forpligtet til at give meddelelse én gang samt spørgsmålet om efterfølgende behandling til nye formål, at være identiske med, hvad der følger af persondatalovens § 28, stk. 1, nr. 1 og 2, hvorfor der, i forhold til forståelse heraf, henvises til behandlingen af samme i afsnit 4.3. om oplysningspligt ved indsamling af oplysninger hos den registrerede.

Derudover kan der i medfør af persondatalovens § 29, stk. 1, nr. 3, gives en række yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysninger er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser. Bestemmelsen nævner i litra a–c, at sådanne yderligere oplysninger f.eks. kan være hvilken type oplysninger, det drejer sig om, kategorierne af modtagere samt om reglerne i indsigt i og berigtigelse af de oplysninger, der vedrører den registrerede.

Det følger af bemærkningerne, at det skal afgøres konkret i det enkelte tilfælde om og i givet fald, hvilke yderligere oplysninger der skal gives, og at oplistning i litra a–c ikke er udtømmende, hvorfor der kan påhvile den dataansvarlige en pligt til at give den registrerede andre oplysninger.

[361] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit2.2.1.
[362] Udtalelse om oplysningspligt i forbindelse med overvågning foretaget af et forsikringsselskab, Datatilsynets j.nr. 2012-213-0047.

I forhold til litra a om, *hvilken type oplysninger det drejer sig om*, følger det af bemærkningerne til persondataloven, at der ikke påhviler den dataansvarlige en pligt til at give den registrerede meddelelse om, hvilke konkrete oplysninger, der er indsamlet om den pågældende.[363] Det er alene *typen* af oplysninger, der i givet fald skal oplyses om. Såfremt den registrerede ønsker at få at vide, hvilke konkrete oplysninger, der er indsamlet, må der søges om indsigt efter reglerne i persondatalovens § 31.

For så vidt angår kategorierne af modtagere samt reglerne om indsigt i og berigtigelse af de oplysninger, der vedrører den registrerede, henvises til behandlingen af samme i afsnit 4.3. om oplysningspligt ved indsamling af oplysninger hos den registrerede.

4.4.2.2. Persondatalovens § 29, stk. 2

Det fremgår af persondatalovens § 29, stk. 2, at bestemmelsen i stk. 1 ikke gælder, hvis den registrerede allerede er bekendt med de i nr. 1–3 nævnte oplysninger, eller hvis registreringen eller videregivelsen udtrykkeligt er fastsat ved lov eller bestemmelser fastsat i henhold til lov. Lignende undtagelser kan findes i databeskyttelsesdirektivets artikel 11.

Bestemmelsen i persondatalovens § 29, stk. 2, 1. led, har en identisk ordlyd med bestemmelsen i persondatalovens § 28, stk. 2. Der må ligesom ved persondatalovens § 28, stk. 2, anlægges en konkret vurdering af omstændighederne omkring indsamlingen af oplysningerne. I modsætning til, hvad der følger ovenfor om persondatalovens § 28, stk. 2, vil den dataansvarlige ofte ikke kunne lægge til grund, at den registrerede allerede er bekendt med de oplysninger, som den dataansvarlige er forpligtet til at meddele.[364]

Det følger af bemærkningerne til persondataloven, at det ofte vil være vanskeligt for den dataansvarlige i praksis at afgøre, hvorvidt den registrerede allerede er bekendt med de yderligere oplysninger, som den dataansvarlige efter omstændighederne er forpligtet til at meddele i henhold til bestemmelsen i stk. 1, nr. 3. I de tilfælde hvor den dataansvarlige eller dennes repræsentant er i tvivl herom, forudsættes det, at der gives den registrerede meddelelse i overensstemmelse med stk. 1.[365] De anførte forhold betyder, at den nye dataansvarlige enten må vide, at den tidligere dataansvarlige har opfyldt sin oplysningspligt efter persondatalovens § 28, eller at en af de andre undtagelsesbestemmelser finder anvendelse, førend denne nye dataansvarlige fritages fra oplysningspligten efter persondatalovens § 29.

[363] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 29.
[364] Persondataloven med kommentarer (2015), s. 479.
[365] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 29.

Derudover kan der undtages fra oplysningspligten i medfør af persondatalovens § 29, stk. 2, 2. led, såfremt *registreringen eller videregivelsen udtrykkeligt er fastsat i lov eller bestemmelser fastsat i henhold til lov*. Det følger af bemærkningerne til persondataloven, at pligten eller retten til at registrere eller videregive oplysninger for det første kan følge af lov i formel forstand. Dette vil bl.a. være tilfældet for så vidt angår reglerne i arkivloven og lov om Danmarks Statistik. Endvidere vil pligten eller retten til at registrere eller videregive oplysninger kunne følge af administrative retsforskrifter såsom anordninger og bekendtgørelser. Det skal være udtrykkeligt fastsat, at der kan eller skal ske registrering eller videregivelse af oplysninger.[366]

I kravet om udtrykkelighed ligger, at det ikke må give anledning til tvivl, hvorvidt det i lovgivningen er fastsat, at den dataansvarlige skal foretage registrering eller videregivelse af de indsamlede oplysninger. Derfor kan det ikke antages, at en generel bemyndigelse til at fastsætte nærmere regler for administrationen af et bestemt sagsområde, herunder en forretningsorden, er fornøden hjemmel til at fravige oplysningspligten, idet lovgiver ikke har haft lejlighed til at forholde sig til, om bemyndigelsen også skulle gælde fravigelse af de grundlæggende rettigheder, som en registreret har efter persondataloven.[367]

I sag C-201/14, Bara, dom af 1. oktober 2015, havde en offentlig myndighed videregivet personoplysninger til en anden offentlig myndighed, der havde foretaget behandling af disse personoplysninger, uden at nogen af myndighederne havde oplyst de registrerede om videregivelse eller behandling.

EU-Domstolen udtalte i præmis 37 og 45, om undtagelsen i databeskyttelsesdirektivets artikel 11, stk. 2, der vedrører videregivelse, der udtrykkeligt er fastsat i lov, at det ikke var tilstrækkeligt for at kunne fritages fra oplysningspligten, at fastlæggelsen af de oplysninger, der måtte videregives såvel som retningslinjerne for videregivelse af disse oplysninger, var sket gennem en protokol indgået mellem to myndigheder, der ikke var blevet bekendtgjort officielt, selvom det i en national lov var fastlagt, at en række nødvendige oplysninger skulle overføres i medfør af protokollen.

Derudover må kravet til udtrykkelighed i øvrigt fastlægges gennem tilsynsmyndighedernes praksis. Af denne følger det, at det som hovedregel kun vil være i de tilfælde, hvor der er tale om en egentlig indberetningspligt, at kravet om udtrykkelighed i § 29, stk. 2, 2. led, er opfyldt. I disse tilfælde vil det være klart for den registrerede (gennem bekendtgørelse i

[366] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 29.
[367] Persondataloven med kommentarer (2015), s. 480-481, hvor Datatilsynet udtalelse om skattekontrollovens § 6 E omtales, Datatilsynet j.nr. 2000-321-0047.

Lovtidende), at der vil blive videregivet oplysninger om vedkommende til f.eks. en anden myndighed. Endvidere vil § 29, stk. 2, 2. led, være opfyldt, hvor det udtrykkeligt fremgår, at der vil blive indhentet oplysninger, så det er klart, at den indhentende myndighed eller lignende vil registrere oplysninger. Det vil således ikke være tilstrækkeligt, at loven hjemler en eventuel mulighed til at indhente/registrere eller videregive oplysninger, da det ikke efter reglerne vil være klart for de registrerede, at der vil blive registreret eller videregivet oplysninger.[368]

4.4.2.3. Persondatalovens § 29, stk. 3

Det fremgår af persondatalovens § 29, stk. 3, at bestemmelsen i stk. 1 ikke gælder, hvis underretning af den registrerede viser sig *umulig* eller er *uforholdsmæssigt vanskelig*.

Af præambelbetragtning nr. 40 i databeskyttelsesdirektivet følger det, at det ikke er nødvendigt at pålægge en underretningspligt, hvis det viser sig umuligt eller uforholdsmæssigt vanskeligt at underrette den pågældende, hvilket kan være tilfældet i forbindelse med behandlinger i historisk, statistisk eller videnskabeligt øjemed; i denne forbindelse kan der tages hensyn til antallet af registrerede, oplysningernes alder samt de kompensatoriske foranstaltninger, der kan træffes.

Af bemærkninger til persondataloven fremgår det, at der med *uforholdsmæssig vanskelig* fastsættes et proportionalitetsprincip ved vurderingen af, om meddelelse, som foreskrevet i stk. 1, skal gives. Der skal ske en afvejning af på den ene side betydningen af en sådan underretning for den registrerede og på den anden side den arbejdsindsats hos den dataansvarlige, der vil være forbundet med en sådan underretning. I hvilket omfang, underretning af registrerede personer er uforholdsmæssig vanskelig eller endog umulig, skal afgøres i den enkelte situation. Der skal i den forbindelse bl.a. lægges vægt på antallet af registrerede, oplysningernes alder samt de kompensatoriske foranstaltninger, f.eks. offentlige oplysningskampagner, der eventuelt måtte blive truffet af den dataansvarlige. Endvidere må det tillægges betydning, hvor betydelige de interesser er, af hensyn til hvilke oplysningerne behandles, og hvor indgribende det er for den enkelte, at der foretages behandling af oplysninger om vedkommende.[369]

Det følger af Datatilsynets vejledning, at denne proportionalitetsvurdering bl.a. vil kunne være relevant med hensyn til eventuelle bipersoner, om hvem der behandles personoplysninger. Uanset at bipersoner som udgangspunkt har de samme rettigheder efter persondata-

[368] Sag vedrørende oplysningspligt i forbindelse med Arbejdsdirektoratets rådighedstilsyn, Datatilsynets j.nr. 2004-321-0316.
[369] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 29.

loven som andre registrerede personer, skal der – på baggrund af de ovennævnte momenter – for hver enkelt behandling af oplysninger om bipersoner tages stilling til, om oplysningspligten skal opfyldes over for den pågældende. En sådan vurdering vil i almindelighed falde ud til, at eventuelle indsamlede eller registrerede oplysninger om bipersoner er uden betydning for de pågældende i forbindelse med den behandling af personoplysninger, som den dataansvarlige foretager. Dette vil bl.a. være tilfældet, hvis f.eks. en dataansvarlig kommune indhenter oplysninger om en person og i samme forbindelse anmoder vedkommende om oplysninger om andre personer, f.eks. familiens læge angivet med navn og konsultationsadresse, personens hjemmehjælper eller lignende personer. For denne situation gælder det, at behandlingen ikke vil have konsekvenser for vedkommende biperson, hvorfor der normalt ikke vil skulle gives underretning efter lovens § 29, stk. 1.[370] Derudover følger det af bemærkningerne til persondataloven, at det ud fra en proportionalitetsbetragtning normalt vil være uforholdsmæssigt vanskeligt for f.eks. dataansvarlige domstole at underrette bipersoner om, at der indsamles oplysninger om dem i forbindelse med behandlingen af en civil retssag.[371]

Det forudsættes endvidere i bemærkningerne til persondataloven, at der efter bestemmelsen kun i særdeles begrænset omfang vil påhvile dataansvarlige, der foretager behandling af oplysninger i statistisk øjemed eller til historiske eller videnskabelige forskningsformål, en oplysningspligt over for de registrerede personer. Det samme forudsættes med hensyn til den behandling af oplysninger, som sker i retsinformationssystemer.[372] Det har i den forbindelse betydning, at der er indsat bestemmelser i persondataloven, der medfører, at de omhandlede oplysninger ikke senere må behandles til andet formål end det oprindeligt indsamlede, jf. persondatalovens § 9, stk. 2, og § 10, stk. 2. Dette betyder, at de registrerede personer kun i meget ringe omfang vil blive berørt af, at der behandles oplysninger om dem.

Det vil være af betydning, om behandling af oplysninger foretages som led i enkeltsagsbehandling, eller om behandlingen foretages i en række identiske sager, eventuelt som led i massesagsbehandling. Såfremt der er tale om enkeltsagsbehandling, vil der være en formodning for, at det ikke vil være uforholdsmæssigt vanskeligt at opfylde oplysningspligten, navnlig ikke hvis opfyldelsen heraf kan ske i forbindelse med iværksættelsen af andre

[370] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.3.3.
[371] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 29.
[372] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 29.

sagsbehandlingsskridt mv. over for den registrerede. Er der tale om et større antal identiske sager, vil det ofte kunne være uforholdsmæssigt vanskeligt at opfylde oplysningspligten.[373]

Fra Datatilsynets praksis kan nævnes en sag, hvor Arbejdsdirektoratet bl.a. anmodede Datatilsynet om at få oplyst, hvorvidt Arbejdsdirektoratet skulle opfylde oplysningspligten i persondatalovens § 29 i forbindelse med gennemførelse af direktoratets tilsyn med kommunernes rådighedsvurderinger for kontant- og starthjælpsmodtagere mv., eller om undtagelsen i § 29, stk. 2, 2. led, kunne finde anvendelse. Arbejdsdirektoratet havde oplyst, at tilsynet dels bestod af stikprøvekontrol, hvor sagerne blev indhentet til direktoratet, dels af tilsynsbesøg i kommunerne, hvor de fleste sager forventedes behandlet under besøget. Der blev ca. 2.500 inddragede sager om året i rådighedskontrol. Spørgsmålet om oplysningspligt opstod alene i forhold til de sager, som direktoratet indkaldte eller hjemtog til gennemgang i direktoratet. Tilsynet ville alene være en vurdering af, om kommunen havde overholdt gældende regler. Tilsynet ville ikke have nogen umiddelbar konsekvens for ydelsesmodtageren. Sagen kunne kun ændres i forhold til borgeren, hvis kontrollen viste, at der var tale om en forkert bebyrdende afgørelse.

Det var Datatilsynets umiddelbare vurdering, at betingelserne for at fravige oplysningspligten med hjemmel i § 29, stk. 3, ikke kunne anses for opfyldt i det konkrete tilfælde. Datatilsynet lagde herved navnlig vægt på omfanget og karakteren af de oplysninger om borgeren, som Arbejdsdirektoratet indhentede og registrerede i forbindelse med rådighedstilsynet, og at direktoratets behandling kunne føre til ændringer i forhold til borgeren, hvis der var tale om en forkert bebyrdende afgørelse. I vurderingen havde Datatilsynet endvidere lagt vægt på formålet med oplysningspligten og det forhold, at Arbejdsdirektoratet oprettede en sag for hver enkelt borger, hvis sag indgik i rådighedstilsynet. Endelig havde Datatilsynet ikke grundlag for at antage, at det ville være forbundet med uforholdsmæssig stor arbejdsindsats at underrette de omhandlede personer.[374]

4.4.3. Databeskyttelsesforordningen

4.4.3.1. Databeskyttelsesforordningens artikel 14, stk. 1

Det fremgår af forordningens artikel 14, stk. 1, at den dataansvarlige, hvis personoplysninger ikke er indsamlet hos den registrerede, giver den registrerede de oplysninger, der følger af bestemmelsens litra a–f.

For så vidt angår forordningens artikel 14, stk. 1, litra a, b, c, e og f, er ordlyden af disse bestemmelser identisk med, hvad der følger af forordningens artikel 13, stk. 1, litra a, b, c,

[373] Persondataloven med kommentarer (2015), s. 485.
[374] Sag vedrørende oplysningspligt i forbindelse med Arbejdsdirektoratets rådighedstilsyn, Datatilsynets j.nr. 2004-321-0316.

e og f, hvorfor der henvises til behandlingen af disse i afsnit 4.3. om oplysningspligt ved indsamling af oplysninger hos den registrerede.

4.4.3.1.1. Databeskyttelsesforordningens artikel 14, stk. 1, litra d
Det fremgår af forordningens artikel 14, stk. 1, litra d, at den dataansvarlige skal give den registrerede meddelelse om *de berørte kategorier af personoplysninger.*

Der er tale om en sproglig ændring i forhold til databeskyttelsesdirektivets artikel 11, stk. 1, litra c, hvoraf det fremgår, at den registrerede skal oplyses om, *hvilken type oplysninger det drejer sig om.*

EU-Domstolen udtalte i Bara-dommen, at artikel 11, stk. 1, litra b og c, i databeskyttelsesdirektivet indebærer, at de registrerede, som er berørt af behandlingen af oplysningerne, skulle være blevet underrettet om formålene med den pågældende behandling og *de berørte kategorier af personoplysninger*.

Det følger af det forhold, at den registrerede skal vide, hvilke oplysninger, der behandles om den pågældende, at denne fra den oprindelige dataansvarlige skal oplyses om kategorierne af eventuelle modtagere. Af den grund følger det samtidig, at den nye dataansvarlige skal oplyse om, hvilke kategorier af personoplysninger, som denne har modtaget fra den oprindelige dataansvarlige.

Forordningens artikel 14, stk. 1, litra d, må ses som en videreførelse af gældende ret.

4.4.3.2. Databeskyttelsesforordningens artikel 14, stk. 2
Det fremgår af forordningens artikel 14, stk. 2, at den dataansvarlige, hvis personoplysninger ikke er indsamlet hos den registrerede, giver den registrerede følgende oplysninger, der er nødvendige for at sikre en rimelig og gennemsigtig behandling. Disse yderligere oplysninger følger af bestemmelsens litra a–g.

Opdelingen i forordningen af artikel 14 i en stk. 1, med oplysninger, der altid *skal* meddeles den registrerede, og en stk. 2, med oplysninger, der er *nødvendige for at sikre en rimelig og gennemsigtig behandling*, må betyde, at den dataansvarlige i medfør af stk. 2 skal foretage en konkret vurdering af, om der skal gives den registrerede yderligere oplysninger, end hvad der allerede kræves i medfør af artikel 14, stk. 1.

Forordningens artikel 14, stk. 2, litra a–e og g, er identisk med, hvad der følger af forordningens artikel 13, stk. 1, litra d, og stk. 2, litra a–d og f, hvorfor der henvises til behand-

ling af samme i afsnit 4.3. om oplysningspligt ved indsamling af oplysninger hos den registrerede.

4.4.3.2.1. Databeskyttelsesforordningens artikel 14, stk. 2, litra f
Det fremgår af forordningens artikel 14, stk. 2, litra f, at den dataansvarlige skal foretage en vurdering af, om det er nødvendigt for at sikre en rimelig og gennemsigtig behandling, at den registrerede meddeles om *hvilken kilde personoplysningerne hidrører fra, og eventuelt hvorvidt de stammer fra offentligt tilgængelige kilder.*

Det følger af præambelbetragtning nr. 61 i databeskyttelsesforordningen, at hvis den registrerede ikke kan informeres om personoplysningers oprindelse, fordi der er anvendt forskellige kilder, bør der gives generelle oplysninger.

Der findes ikke i gældende ret bestemmelser, der specifikt forpligter den dataansvarlige til at oplyse om de indsamlede oplysningers kilde. Det forhold, at det med forordningen er gjort til et specifikt krav at oplyse den registrerede, såfremt det af den dataansvarlige vurderes at være nødvendigt for at sikre en rimelig og gennemsigtig behandling, om hvilken kilde oplysningerne hidrører fra, er således en udvidelse af gældende ret.

4.4.3.3. Databeskyttelsesforordningens artikel 14, stk. 3
Forordningens artikel 14, stk. 3, litra a–c fastsætter den maksimale frist for, hvornår den dataansvarlige skal give den registrerede de oplysninger, som er omhandlet i stk. 1 og 2. Bestemmelsen fastsætter tre forskellige frister afhængigt af, hvad personoplysningerne skal anvendes til.

Bestemmelsens litra a, fastsætter, at den dataansvarlige *inden for en rimelig frist* efter indsamlingen af personoplysningerne, men senest *inden for en måned* under hensyn til de specifikke forhold, som personoplysninger er behandlet under, skal give de oplysninger, der er omhandlet i artikel 14, stk. 1 og 2.

Der er ingen indikationer af, at indsættelsen af *inden for rimelig frist efter indsamlingen* i stedet for *ved registreringen* i databeskyttelsesdirektivets artikel 11, er sket med ønske om at ændre på den gældende retstilstand, hvorefter den dataansvarlige bør give den registrerede meddelelse så tidligt som muligt. *Ved registreringen* er i dansk ret blevet fortolket til, at oplysningspligten i almindelighed vil skulle opfyldes inden for 10 dage, hvilket antages at kunne indeholdes i forordningens krav om, at dette skal ske *inden for rimelig frist efter indsamlingen.* Denne forståelse stemmer overens med forordningens generelle mål om åbenhed og gennemsigtighed over for den registrerede.

Det er imidlertid nyt, at der nu er fastsat en maksimal frist for, hvornår indsamling af personoplysninger skal oplyses den registrerede. Dette medfører næppe til de store ændringer af gældende ret, idet det må antages, at der sjældent i dag vil forekomme situationer, hvor en dataansvarlig kan komme med en legitim begrundelse for, at det skal tage mere end én måned at oplyse den registrerede om indsamlingen af personoplysninger.

Bestemmelsens litra b specificerer, at hvis personoplysningerne skal bruges til at kommunikere med den registrerede, så skal der gives meddelelse senest på tidspunktet for den første kommunikation med den registrerede.

Der følger ikke en lignende specificering af oplysningspligten i forbindelse med kommunikation med den registrerede i gældende ret. Det følger dog af kravet om, at den registrerede gives meddelelse så tidligt som muligt, at den dataansvarlige ikke kan undlade at opfylde oplysningspligten over for den registrerede, første gang denne kontakter den registrerede.

Bestemmelsens litra c specificerer, at hvis personoplysningerne er bestemt til videregivelse til en anden modtager, så skal der gives meddelelse senest, når personoplysningerne videregives første gang. Forordningens bestemmelse har en næsten identisk ordlyd med databeskyttelsesdirektivets artikel 11, som persondatalovens § 29 er baseret på, hvorfor der må formodes at være samme indholdsmæssige betydning i bestemmelserne.

Ordlyden i databeskyttelsesdirektivets artikel 11 om, at den dataansvarlige, *senest når oplysningerne første gang videregives til tredjemand,* skal opfylde oplysningspligten, stemmer overens med ordlyden i forordningen om, *senest når personoplysningerne videregives første gang.*

Derudover nævner forordningen, at det er, hvis personoplysningerne er *bestemt til videregivelse til en anden modtager,* at der skal gives meddelelse til den registrerede. Det følger allerede af gældende ret i medfør af kravet om, at der skal oplyses om modtagerne eller kategorierne af modtagere i databeskyttelsesdirektivets artikel 11, stk. 1, stk. litra c, at den dataansvarlige på tidspunktet for indsamlingen skal tage stilling til, om personoplysningerne skal videregives.

4.4.3.4. Databeskyttelsesforordningens artikel 14, stk. 4

Det følger af forordningens artikel 14, stk. 4, at hvis den dataansvarlige agter at viderebehandle personoplysningerne til *et andet formål* end det, hvortil de er indsamlet, giver den dataansvarlige forud for denne viderebehandling den registrerede oplysninger om dette andet formål og andre relevante yderligere oplysninger, jf. stk. 2.

Det følger af gældende ret, som gengivet under afsnit 4.3. om oplysningspligt ved indsamling hos den registrerede, at de krav, der skal stilles til formålsangivelsen vil bero på en vurdering af de konkrete omstændigheder omkring behandlingen af oplysningerne, og at oplysninger *i almindelighed* endvidere vil kunne behandles (benyttes) til andre, efterfølgende saglige formål, uden at den dataansvarlige på ny skal give den registrerede meddelelse, hvis behandlingen ikke er uforenelig med det eller de formål, som oprindeligt er oplyst til den registrerede i forbindelse med opfyldelse af oplysningspligten. Det er kun *i særlige tilfælde*, at der vil påhvile den dataansvarlige en pligt til efterfølgende at oplyse om (nye) behandlingsformål, som ikke er omfattet af den oprindelige meddelelse, og som aktualiseres efter tidspunktet for indsamlingen af oplysninger.

Forordningen fastsætter, at der skal oplyses om, at den dataansvarlige agter at viderebehandle personoplysninger, når dette sker til et *andet formål*. Efter en ordlydsfortolkning må denne ændring efter omstændighederne udvide området for, hvornår der skal gives en registreret meddelelse om viderebehandling af den pågældendes personoplysninger, i og med, at det efter forordningen vil være den blotte omstændighed, at formålet er et andet, der udløser ny oplysningspligt. Efter gældende ret har den dataansvarlige allerede skulle foretage en vurdering af en viderebehandlings uforenelighed med de allerede oplyste formål. Denne vurdering skal stadig foretages i medfør af forordningen, hvor betydningen af den ændrede ordlyd efter omstændighederne bliver, at den dataansvarlige oftere vil skulle oplyse den registrerede, når der foretages viderebehandling.

For så vidt angår kravet om at oplyse den registrerede om *andre relevante yderligere oplysninger,* må den dataansvarlige i forbindelse med en viderebehandling foretage en konkret vurdering af, om det er nødvendigt for at sikre en *rimelig* og *gennemsigtig* behandling, at der gives den registrerede en række yderligere oplysninger, der følger af artikel 14, stk. 2. Det er ved foretagelsen af denne vurdering oplagt at vurdere, om den registrerede allerede er bekendt med oplysningerne, hvorfor en meddelelse ikke er nødvendig, jf. artikel 14, stk. 5, litra a.

4.4.3.5. Databeskyttelsesforordningens artikel 14, stk. 5

Forordningen fastsætter i artikel 14, stk. 5, litra a-d, en række undtagelser til den dataansvarliges oplysningspligt.

For så vidt angår forordningens artikel 14, stk. 5, litra a, om hvorvidt den registrerede allerede er bekendt med oplysningerne, er ordlyden identisk med, hvad der følger af forordningens artikel 13, stk. 4, hvorfor der henvises til behandlingen af denne i afsnit 4.3. om oplysningspligt ved indsamling af oplysninger hos den registrerede.

Af bestemmelsens litra b, 1. pkt., undtages meddelelse af oplysninger, hvis denne viser sig at være umulig eller vil kræve uforholdsmæssigt stor indsats, navnlig i forbindelse med behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål underlagt de betingelser og garantier, der er omhandlet i artikel 89, stk. 1, eller i det omfang den forpligtelse, der er omhandlet i nærværende artikels stk. 1, sandsynligvis vil gøre det umuligt eller i alvorlig grad vil hindre opfyldelse af formålene med denne behandling.

Det følger af databeskyttelsesdirektivets artikel 11, stk. 2, som persondatalovens § 29, stk. 2, er baseret på, at der ikke skal ske underretning af den registrerede, navnlig ikke når behandling foretages i *statistisk* øjemed eller til *historiske* eller *videnskabelige forskningsformål,* samt hvis underretning af den registrerede viser sig *umulig* eller *uforholdsmæssigt vanskelig*.

Det følger bl.a. af forordningens præambelbetragtning nr. 62, at der i forbindelse med vurderingen af, om der kan undtages fra underretningspligten, *bør* tages hensyn til antallet af registrerede, oplysningernes alder og eventuelle fornødne garantier, der er stillet.

Betragtningen ses umiddelbart at udgøre en sproglig ændring i forhold til præambelbetragtning nr. 40 i databeskyttelsesdirektivet, hvor det fremgår, at hvis det viser sig umuligt eller uforholdsmæssigt vanskeligt at underrette den pågældende, hvilket kan være tilfældet i forbindelse med behandlinger i historisk, statistisk eller videnskabeligt øjemed, *kan* der i den forbindelse tages hensyn til antallet af registrerede, oplysningernes alder samt de kompensatoriske foranstaltninger, der kan træffes.

For så vidt angår vurderingen af, om underretningen "vil kræve en uforholdsmæssigt stor indsats", er der imidlertid tale om en sproglig ændring i forhold til direktivets artikel 11, stk. 2, hvor underretning kan undtages, såfremt det "er uforholdsmæssigt vanskelig".

Disse ændringer i ordlyden i forordningens artikel 14, stk. 5, litra b, og præambelbetragtning nr. 62, kan umiddelbart tale i retning af, at der kan være en indholdsmæssig ændring i undtagelsesmuligheden efter databeskyttelsesdirektivet og forordningen.

Det, at der ikke skal ske underretning, såfremt "det vil kræve en uforholdsmæssig stor indsats", taler i retning af, at der er tale om et subjektivt frem for et objektivt begreb, når det skal vurderes, om oplysningspligten skal efterleves i et givet tilfælde som følge af, at det viser sig, at det vil kræve en uforholdsmæssig stor indsats. Denne umiddelbare antydning af en ændring i begrebets karakter kan betyde, at en dataansvarlig formentlig potentielt vil

kunne undlade at foretage underretning, selv hvor en efterlevelse i realiteten godt kan lade sig gøre, men hvor det vil kræve en uforholdsmæssig stor indsats fra den dataansvarlige.

Der kan således med ordlyden i forordningens artikel 14, stk. 5, litra b, fortolkes en antydning af, at undtagelsesmuligheden udvides i forhold til databeskyttelsesdirektivet og persondataloven.

For så vidt angår vurderingen af, om der er tale om behandling, der foretages til videnskabelige eller historiske forskningsformål eller til statistiske formål, der overholder de fornødne garantier for registreredes rettigheder og frihedsrettigheder, der følger af forordningens artikel 89, stk. 1, ses forordningens undtagelsesmuligheder at være en videreførelse af gældende ret.

For så vidt angår undtagelsen til behandling til arkivformål i samfundets interesse, følger det af persondatalovens § 14, at der kan ske overførsel til arkiv af de oplysninger, der er omfattet af reglerne i arkivloven. Derudover gælder, at hvis det udtrykkeligt følger af arkivloven, at oplysninger skal videregives, vil undtagelsen om *udtrykkeligt fastsat ved lov* i persondatalovens § 29, stk. 2, finde anvendelse.

Forordningen må derved antages at udvide undtagelserne, ved at det nu direkte fremgår, at der kan undtages fra oplysningspligten *i forbindelse med behandling til arkivformål i samfundets interesse,* hvis det viser sig umulig eller vil kræve en uforholdsmæssig stor indsats.

Derudover følger det af forordningen, at underretning ikke er nødvendig, såfremt det *sandsynligvis vil gøre det umuligt eller i alvorlig grad vil hindre opfyldelse af formålene med denne behandling.* Det vil f.eks. være tilfældet, hvis en underretning kan skade en efterforskning og forfølgelse af lovovertrædelser.

Hvis den dataansvarlige ikke underretter den registrerede som følge af, at formålet med behandling vil forspildes eller hindres, må den dataansvarlige, når dette ikke længere er tilfældet, opfylde sin oplysningspligt over for den registrerede.

Det følger af Datatilsynets praksis i ovennævnte sag om et forsikringsselskab, at forsikringsselskabets oplysningspligt, under hensyn til formålet med registreringen i den konkrete sag – at indsamle oplysninger om klager uden hendes vidende – først skulle opfyldes umiddelbart efter afslutningen af observationerne af klager.[375]

[375] Udtalelse om oplysningspligt i forbindelse med overvågning foretaget af et forsikringsselskab, Datatilsynets j.nr. 2012-213-0047.

Af forordningens artikel 14, stk. 5, litra b, 2. pkt., følger det, at såfremt den dataansvarlige anvender en af de ovennævnte undtagelser i litra b, 1. pkt., skal der træffes passende foranstaltninger for at beskytte den registreredes rettigheder og frihedsrettigheder samt legitime interesser, herunder ved at gøre oplysninger offentligt tilgængelige.

Bestemmelsen udspecificerer, at i den situation, at den registrerede ikke er vidende om, at der er indsamlet personoplysninger om denne af en dataansvarlig, og derfor ikke selv har mulighed for at varetage sine interesser, skal den dataansvarlige træffe passende foranstaltninger. Det følger i lighed hermed af databeskyttelsesdirektivets artikel 11, stk. 2, 2. pkt., at medlemsstaterne, i de ovennævnte undtagelsestilfælde, fastsætter de fornødne garantier.

Dette krav om passende foranstaltninger må i mange tilfælde kunne opfyldes ved, at den dataansvarlige f.eks. på sin hjemmeside generelt oplyser om det, der fremgår af artikel 14, stk. 1-2.

Af bestemmelsens litra c undtages meddelelse af oplysninger, hvis indsamling eller videregivelse udtrykkelig er fastsat i EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt, og som fastsætter passende foranstaltninger til beskyttelse af den registreredes legitime interesser.

Det følger af databeskyttelsesdirektivets artikel 11, stk. 2, at der ikke skal gives underretning, såfremt *registreringen eller videregivelsen af oplysninger udtrykkeligt er fastsat ved lov*. Af persondatalovens § 29, stk. 2, følger det, at der kan undtages fra oplysningspligten, såfremt *registreringen eller videregivelsen er fastsat ved lov eller bestemmelser i henhold til lov*.

Der ses med litra c ikke at være ændringer i forhold til gældende ret, herunder de gældende krav til udtrykkelighed.

Af bestemmelsens litra d undtages meddelelse af oplysninger, hvis personoplysninger skal forblive fortrolige som følge af tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret, herunder lovbestemt tavshedspligt.

Med bestemmelsen i litra d har EU-lovgiver tilsyneladende indført en undtagelse, der svarer til persondatalovens § 32, stk. 2, om indsigtsretten med henvisningen heri til offentlighedslovens § 35, der indebærer, at der ikke er indsigt i sager omfattet af særlige bestemmelser om tavshedspligt, såsom skatteforvaltningslovens § 17. Samme udtagelse ses således med henvisningen til "lovbestemte tavshedspligt" i forordningens artikel 14, stk. 5, litra d, at være indført vedrørende oplysningspligten efter artikel 14 – en undtagelse, der

ikke er gældende i forvejen, da persondatalovens § 29, stk. 2-3, og § 30 om undtagelser fra oplysningspligten ikke indeholder en undtagelsesmulighed svarende til persondatalovens § 32, stk. 2.

4.4.4. Overvejelser

Vedrørende databeskyttelsesforordningens artikel 14, stk. 1, følger det allerede af gældende ret, at der skal gives meddelelse om identitet på den dataansvarlige samt formålene med den behandling, der foretages. Derudover følger det også af gældende ret, at der skal foretages en vurdering af, om der skal gives oplysning om eventuelle modtagere eller kategorier af modtagere samt om de berørte kategorier af personoplysninger.

Forordningens artikel 14, stk. 1, udvider området for de oplysninger, der altid skal gives, når personoplysninger behandles om den registrerede ved at pålægge den dataansvarlige en pligt til altid at give meddelelse om kontaktoplysninger på en eventuel databeskyttelsesrådgiver, kontaktoplysninger for den dataansvarlige og dennes repræsentant, retsgrundlaget for behandlingen samt, hvis det er relevant, overførsler i medfør af forordningens artikel 45–47 og artikel 49.

Vedrørende databeskyttelsesforordningens artikel 14, stk. 2, følger det allerede af gældende ret, at den dataansvarlige skal foretage en vurdering af, om der skal oplyses om reglerne om indsigt i og berigtigelse samt sletning af oplysninger og om retten til at tilbagekalde et samtykke.

Forordningens artikel 14, stk. 2, udvider området for de oplysninger, der, efter en konkret vurdering, skal meddeles den registrerede ved at specificere, at der skal foretages en vurdering af tidsperioden for opbevaring af oplysninger, de legitime interesser, der forfølges, retten til begrænsning af behandling af oplysninger, retten til dataportabiliet, retten til at indgive klage til en tilsynsmyndighed, personoplysningernes kilde samt om forekomsten af automatiske afgørelser.

Forordningens artikel 14, stk. 3, fastsætter, som noget nyt, en maksimal frist for, hvornår indsamlingen af personoplysninger skal oplyses den registrerede.

Det følger af forordningens artikel 14, stk. 4, at området for den dataansvarliges oplysningspligt over for den registrerede udvides, ved at denne i medfør af forordningen gælder, når der foretages viderebehandling af personoplysninger til andre formål end det, hvortil personoplysningerne er indsamlet.

Der ses endvidere en umiddelbar antydning af, at undtagelsesmuligheden i forordningens artikel 14, stk. 5, litra b, om meddelelse, der vil kræve en uforholdsmæssig stor indsats udvides i forhold til gældende ret.
Det er nyt, at der i medfør af artikel 14, stk. 5, litra d, kan undtages fra oplysningspligten, som følge af tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret, herunder lovbestemt tavshedspligt.

Det skal endelig bemærkes, at standardiserede ikoner i medfør af artikel 12, stk. 7 og 8, kan anvendes af den dataansvarlige for at opfylde oplysningspligten i artikel 13 og 14. For en nærmere behandling af artikel 12, stk. 7 og 8 henvises til afsnit 4.2.

Forordningen udvider med artikel 14 generelt omfanget af den dataansvarliges oplysningspligt. Den dataansvarlige skal dog allerede foretage en række vurderinger i forbindelse med behandling af oplysninger efter de generelle behandlingsregler i medfør af persondatalovens kapitel 4.

4.5. Indsigtsretten, artikel 15

4.5.1. Præsentation

Reglerne om den registreredes indsigtsret er fastsat i persondatalovens kapitel 9.

Bestemmelserne i kapitel 9 er baseret på artikel 12, litra a, og artikel 13 i databeskyttelsesdirektivet.

Databeskyttelsesforordningens artikel 15 omhandler tilsvarende reglerne om den registreredes indsigtsret.

4.5.2. Gældende ret

Reglerne om den registreredes indsigtsret (egenacces) er fastsat i persondatalovens kapitel 9 (§§ 31-34). Reglerne, der gælder for både offentlige myndigheder og private virksomheder mv., er kun i begrænset omfang ændret i forhold til reglerne om registerindsigt i den tidligere gældende registerlovgivning. Ændringerne er navnlig foretaget for at sikre en korrekt gennemførelse af bestemmelserne i artikel 12, litra a, og artikel 13 i databeskyttelsesdirektivet.[376]

[376] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.

4.5.2.1. Persondatalovens §§ 31, stk. 1 og 33 – den registreredes indsigtsret
Det fremgår af persondatalovens § 31, stk. 1, at fremsætter en person begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om, 1) hvilke oplysninger der behandles, 2) behandlingens formål, 3) kategorierne af modtagere af oplysningerne og 4) tilgængelig information om, hvorfra disse oplysninger stammer.

Bestemmelsen er baseret på artikel 12, litra a, i databeskyttelsesdirektivet, hvoraf det fremgår, at medlemsstaterne sikrer enhver registreret ret til hos den dataansvarlige frit og uhindret, med rimelige mellemrum og uden større ventetid eller større udgifter – at få oplyst, om der behandles personoplysninger om den pågældende selv, samt mindst formålene med behandlingen, hvilken type oplysninger det drejer sig om, og modtagerne eller kategorierne af modtagere af oplysningerne – at få meddelt letforståelig information om, hvilke oplysninger der er omfattet af behandlingerne, samt enhver tilgængelig information om, hvorfra disse oplysninger stammer – at få at vide, hvilken logik der ligger bag edb-behandlingen af oplysningerne om den pågældende, i det mindste i forbindelse med edb-baserede afgørelser som omhandlet i artikel 15, stk. 1.

Det fremgår af præambelbetragtning nr. 41 til databeskyttelsesdirektivet, at enhver skal have ret til indsigt i de oplysninger om sig selv, som gøres til genstand for behandling, så den pågældende kan forvisse sig om oplysningernes rigtighed og behandlingens lovlighed. Det fremgår endvidere af samme præambelbetragtning, at af samme årsag skal enhver have ret til at kende den logik, der ligger bag edb-behandlingen af oplysningerne om sig selv, i det mindste i forbindelse med edb-baserede (automatiske) afgørelser, som omhandlet i artikel 15, stk. 1.

Det fremgår endvidere af samme præambelbetragtning, at denne ret ikke må krænke forretningshemmeligheden eller den intellektuelle ejendomsret, navnlig den ophavsret, som programmerne er beskyttet af. Dette må dog ikke resultere i, at den registrerede nægtes alle oplysninger.

Hovedreglen om indsigtsret er efter lovens § 31, stk. 1, at enhver person, som fremsætter begæring herom, har ret til at få meddelelse om en række forhold, herunder bl.a. om der behandles oplysninger om den pågældende, og i givet fald hvilke oplysninger der behandles. Efter bestemmelsen kan der ikke stilles særlige krav til en begæring om indsigt (ege-

nacces), men der vil alligevel kunne opstå en række spørgsmål om begæringen og dens indhold.[377]

Datatilsynet anfører i vejledning om registreredes rettigheder, at efter tilsynets opfattelse er der ikke noget til hinder for, at en registrerets begæring om indsigt i samtlige en myndigheds forvaltningsgrenes oplysninger imødekommes ved indhentelse af bidrag fra de relevante forvaltningsgrene med henblik på en samlet gennemførelse af den registreredes indsigtsret. Den kommunale forvaltning er en enhedsforvaltning.[378]

Det helt klare udgangspunkt er, at der ikke kan stilles særlige formkrav til indsigtsbegæringen. Begæringen kan fremsættes både mundtligt og skriftligt, herunder via e-mail.[379]

Det fremgår af bemærkningerne til persondataloven, at begæringen skal rettes til den dataansvarlige eller dennes repræsentant. Såfremt en registreret person er i tvivl om, hvem der er ansvarlig for de pågældende behandlinger, vil den pågældende eventuelt kunne rette henvendelse herom til vedkommende tilsynsmyndighed.[380]

Det antages, at der ikke er et krav om, at den person, som fremsætter en begæring om indsigt skal kunne give en præcis angivelse af de behandlinger, som vedkommende ønsker indsigt i, og en begæring om indsigtsret kan derfor principielt vedrøre alle de behandlinger, som måtte blive foretaget for den dataansvarlige. I sådanne tilfælde vil der imidlertid ikke være noget til hinder for, at den dataansvarlige oplyser vedkommende om, hvilke behandlinger af oplysninger der foretages, herunder om vedkommende kan være registreret i manuelle registre, med henblik på en afklaring af, hvilke nærmere behandlinger der ønskes indsigt i.[381]

Ifølge lovens § 31, stk. 1, har alle registrerede personer adgang til alle oplysninger om sig selv. Retten til indsigt omfatter både hovedpersoner og bipersoner.[382]

---

[377] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.1.
[378] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.1.2.
[379] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.1.3.
[380] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 31.
[381] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.1.1.
[382] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.2.2.

Det fremgår persondatalovens § 31, stk. 1, nr. 1, at der skal gives den registrerede meddelelse om, hvilke oplysninger om den pågældende, der behandles.

Det fremgår endvidere af bemærkningerne til persondatalovens § 31, stk. 1, nr. 1, at de oplysninger, der efter bestemmelsen skal meddeles den registrerede, er de oplysninger, der behandles på tidspunktet for begæringen, samt oplysninger der er kommet til i perioden frem til, at begæringen ekspederes. Den registrerede har således ikke krav på at få oplyst, hvilke oplysninger der tidligere har været undergivet behandling. Bestemmelsen er dog naturligvis ikke til hinder for, at sådanne ældre oplysninger meddeles.[383]

Det fremgår endvidere af persondatalovens § 31, stk. 1, nr. 2, at der skal gives meddelelse om behandlingens formål.

Det fremgår af bemærkningerne til bestemmelsen, at der heri ikke ligger en forpligtelse for den dataansvarlige til at meddele, hvad oplysningerne nøjagtigt vil skulle bruges til. En generel angivelse af, hvad formålet med behandlingen er, vil være tilstrækkeligt.[384] For så vidt angår den nærmere rækkevidde af kravet om formålsangivelse henvises til afsnit 4.3. om oplysningspligt ved indsamling hos den registrerede.

Herudover fremgår det persondatalovens § 31, stk. 1, nr. 3, at der skal gives meddelelse om kategorierne af modtagere af oplysningerne.

Det er alene modtagerkategorier og ikke de konkrete modtagere, der skal gives oplysning om.[385]

Endvidere fremgår det af persondatalovens § 31, stk. 1, nr. 4, at der skal gives den registrerede tilgængelig information om, hvorfra de oplysninger, der behandles, stammer.

Det fremgår af bemærkninger til persondatalovens § 31, stk. 1, nr. 4, at denne pligt således kun gælder, hvis der foreligger oplysning herom. Der påhviler ikke den dataansvarlige en forpligtelse til at tilvejebringe og opbevare sådanne oplysninger.[386] For den offentlige forvaltnings vedkommende må det i hvert fald for så vidt angår den digitale behandling af afgørelsessager imidlertid antages, at myndigheden som følge af reglerne om notatpligt

[383] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 31.
[384] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 31.
[385] Persondataloven med kommentarer (2015), s. 502.
[386] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 31.

med hensyn til væsentlige sagsbehandlingsskridt oftest vil være i besiddelse af information om, hvorfra oplysningerne i sagen stammer.[387]

Det fremgår af persondatalovens § 33, at en registreret person, der har fået meddelelse efter § 31, stk. 1, ikke har krav på ny meddelelse før 6 måneder efter sidste meddelelse, medmindre der godtgøres en særlig interesse heri.

Det fremgår af Datatilsynets vejledning om registreredes rettigheder vedrørende § 33, at den registrerede således har mulighed for, uanset fristen, at få indsigt f.eks. i tilfælde, hvor den pågældende kan godtgøre, at der siden en tidligere meddelelse om, at der ikke behandles oplysninger om vedkommende, foreligger omstændigheder, der tyder på, at der nu behandles oplysninger om den pågældende. Nævnes kan også den situation, at der er sket væsentlige ændringer i de oplysninger, som behandles, eller af de forhold der behandles oplysninger om. Bestemmelsen i lovens § 33 er naturligvis ikke til hinder for, at den dataansvarlige imødekommer indsigtsbegæringer inden 6 måneder efter en tidligere meddelelse.[388]

4.5.2.2. Persondatalovens § 34, stk. 1 – udgangspunkt om skriftlighed

Det følger af persondatalovens § 34, stk. 1, at meddelelser i henhold til § 31, stk. 1, på begæring skal gives skriftligt. I tilfælde, hvor hensynet til den registrerede taler derfor, kan meddelelse dog gives i form af en mundtlig underretning om indholdet af oplysningerne.

Det fremgår af bemærkningerne til persondataloven, at kravet om skriftlighed indebærer, at oplysningerne skal fremtræde i en sådan form, at de kan læses umiddelbart og uden brug af tekniske hjælpemidler. I de tilfælde, hvor hensynet til den registrerede taler derfor, kan meddelelse af indsigt ske i form af mundtlig underretning om indholdet af oplysningerne. Dette vil bl.a. kunne være tilfældet med hensyn til oplysninger om den registreredes helbredsforhold.[389]

I tilfælde, hvor den registrerede møder personligt op hos den dataansvarlige, bør det søges klarlagt, om den registrerede ønsker skriftligt svar eller en mundtlig underretning om indholdet af oplysningerne.[390]

---

[387] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.2.1.
[388] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.6.5.
[389] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 34.
[390] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.4.

4.5.2.3. Persondatalovens § 32, stk. 1, jf. § 30 – undtagelser til den registreredes indsigtsret

Det fremgår af persondatalovens § 32, stk. 1, som findes i persondatalovens kapitel 9 om registreredes indsigtsret, at bestemmelserne i § 30 finder tilsvarende anvendelse.

Det fremgår af persondatalovens § 30, stk. 1, at bestemmelserne i § 28, stk. 1, og § 29, stk. 1, ikke gælder, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv.

Det fremgår af bemærkninger til persondataloven, at som private interesser, der bl.a. vil kunne begrunde hemmeligholdelse, kan nævnes forretningshemmeligheder, den professionelle tavshedspligt, som læger og advokater skal iagttage, retten til at forberede sit eget forsvar i retssager samt beskyttelse af menneskerettighederne.[391]

Det fremgår endvidere af Datatilsynets vejledning om registreredes rettigheder, at undtagelse på grund af afgørende hensyn til private interesser efter omstændighederne kan gøres af hensyn til forretningshemmeligheder eller af hensyn til beskyttelse af andre personer, som indgår i behandlingen.[392]

Det fremgår af persondatalovens § 30, stk. 2, at undtagelse fra bestemmelserne i § 28, stk. 1, og § 29, stk. 1, tillige kan gøres, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige interesser, herunder navnlig til 1) statens sikkerhed, 2) forsvaret, 3) den offentlige sikkerhed, 4) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv, 5) væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender, og 6) kontrol-, tilsyns- eller reguleringsopgaver, herunder opgaver af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i nr. 3-5 nævnte områder.

Det fremgår af bemærkningerne til persondatalovens § 30, at bestemmelsen fastsætter, at indskrænkning i den dataansvarliges eller dennes repræsentants oplysningspligt kun kan ske på grundlag af en konkret afvejning af de modstående interesser, som er nævnt i be-

[391] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 30.
[392] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.3.4.

stemmelsen. På baggrund af en sådan afvejning vil undtagelse kunne gøres, hvis der er nærliggende fare for, at det offentliges interesser vil lide skade af væsentlig betydning.[393]

Det fremgår endvidere af Datatilsynets vejledning om registreredes rettigheder, at bevisbyrden påhviler den dataansvarlige.[394]

Det fremgår endelig af Datatilsynets vejledning om registreredes rettigheder, at selve afvejningen af de modstående interesser må foretages for hver enkelt oplysning for sig med den virkning, at den registrerede, såfremt afgørende hensyn til private eller offentlige interesser kun gør sig gældende for en del af oplysningerne, som behandles hos den dataansvarlige, skal gøres bekendt med de øvrige oplysninger. Der er ikke efter bestemmelsen adgang til generelt at undtage bestemte former for behandlinger af oplysninger fra indsigtsretten.[395]

I persondatalovens § 32, stk. 2-5, er der endvidere en række yderligere undtagelser, hvorefter den registrerede ikke har indsigtsret.

Der henvises endvidere til afsnit 4.13. om begrænsninger af rettighederne, artikel 23.

4.5.3. Databeskyttelsesforordningen

Det fremgår af Kommissionens forslag til databeskyttelsesforordningen, at artikel 15 omhandler den registreredes ret til indsigt i sine personoplysninger, og at bestemmelsen tager sit udgangspunkt i artikel 12, litra a, i databeskyttelsesdirektivet, idet der tilføjes nye elementer, som har til formål at oplyse de registrerede om opbevaringsperioden samt retten til berigtigelse, sletning og indgivelse af klager.[396]

4.5.3.1. Databeskyttelsesforordningens artikel 15, stk. 1 – den registreredes indsigtsret

Det fremgår af databeskyttelsesforordningens artikel 15, stk. 1, at den registrerede har ret til at få den dataansvarliges bekræftelse på, om personoplysninger vedrørende den pågældende behandles, og i givet fald adgang til personoplysningerne og følgende information:

a) formålene med behandlingen,
b) de berørte kategorier af personoplysninger,

[393] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 30.
[394] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.3.4.
[395] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 3.6.1.
[396] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig).

c) de modtagere eller kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, navnlig modtagere i tredjelande eller internationale organisationer,
d) om muligt det påtænkte tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til fastlæggelse af dette tidsrum,
e) retten til at anmode den dataansvarlige om berigtigelse eller sletning af personoplysninger eller begrænsning af behandling af personoplysninger vedrørende den registrerede eller til at gøre indsigelse mod en sådan behandling,
f) retten til at indgive en klage til en tilsynsmyndighed,
g) enhver tilgængelig information om, hvorfra personoplysningerne stammer, hvis de ikke indsamles hos den registrerede og
h) forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede.

Det fremgår af præambelbetragtning nr. 63, at en registreret bør have ret til indsigt i personoplysninger, der er indsamlet om vedkommende, og til let og med rimelige mellemrum at udøve denne ret med henblik på at forvisse sig om og kontrollere en behandlings lovlighed. Dette omfatter registreredes ret til indsigt i deres helbredsoplysninger, f.eks. data i deres lægejournaler om diagnoser, undersøgelsesresultater, lægelige vurderinger samt enhver behandling og ethvert indgreb, der er foretaget.

Det fremgår endvidere af samme præambelbetragtning, at enhver registreret derfor bør have ret til at kende og blive underrettet om navnlig de formål, hvortil personoplysningerne behandles, om muligt perioden, hvor personoplysningerne behandles, modtagerne af personoplysningerne, logikken der ligger bag en automatisk behandling af personoplysninger, og om konsekvenserne af sådan behandling, i hvert fald når den er baseret på profilering. Hvis det er muligt, bør den dataansvarlige kunne give fjernadgang til et sikkert system, der giver den registrerede direkte adgang til vedkommendes personoplysninger.

Det fremgår endelig af præambelbetragtning nr. 63, at denne ret ikke bør krænke andres rettigheder eller frihedsrettigheder, herunder forretningshemmeligheder eller intellektuel ejendomsret, navnlig den ophavsret, som programmerne er beskyttet af. Denne vurdering bør dog ikke resultere i en afvisning af at give al information til den registrerede. Hvis den dataansvarlige behandler en stor mængde oplysninger om den registrerede, bør den dataansvarlige kunne anmode om, at den registrerede, inden informationen gives, præciserer den information eller de behandlingsaktiviteter, som anmodningen vedrører.

Det fremgår endvidere af præambelbetragtning nr. 64, at den dataansvarlige bør træffe alle rimelige foranstaltninger for at bekræfte identiteten af en registreret, som anmoder om indsigt, navnlig i forbindelse med onlinetjenester og onlineidentifikatorer. Af samme præambelbetragtning fremgår det, at en dataansvarlig ikke bør opbevare personoplysninger alene for at kunne reagere på mulige anmodninger.

Bestemmelsen i databeskyttelsesforordningens artikel 15 stk. 1, bygger som anført på databeskyttelsesdirektivets artikel 12, litra a, som persondatalovens § 31, stk. 1, er baseret på.

Bestemmelserne oplister således nogenlunde tilsvarende de samme fire typer af oplysninger, som den registrerede skal gives meddelelse om efter databeskyttelsesdirektivet og persondataloven, nemlig oplysninger der behandles, behandlingens formål, kategorierne af modtagere af oplysningerne og tilgængelig information om, hvorfra disse oplysninger stammer.

Derudover tilføjes med databeskyttelsesforordningens artikel 15, stk. 1, litra d, e, f og h, nye elementer, der skal gives indsigtsret i.

Ordlyden af databeskyttelsesforordningens artikel 15, stk. 1, ses som udgangspunkt at svare til databeskyttelsesdirektivets artikel 12, litra a, ligesom fortolkningsbidraget i præambelbetragtningerne ses at være i overensstemmelse med, hvad der følger af gældende ret – dog er der i bestemmelsen tilføjet nye elementer, som har til formål at oplyse de registrerede om opbevaringsperioden samt retten til berigtigelse, sletning og indgivelse af klager.

Databeskyttelsesforordningens artikel 15, stk. 1, litra b, har en anden ordlyd end databeskyttelsesdirektivets artikel 12, litra a. Det følger således af forordningens bestemmelse, at der skal gives indsigt i de *berørte kategorier af personoplysninger*, hvorimod det af databeskyttelsesdirektivet følger, at der skal gives indsigt i, *hvilken type oplysninger*, det drejer sig om. Ordlyden i bestemmelserne er således ikke helt identiske, men betydningen af ordene *kategorier* og *type*, må på baggrund af en ordlydsfortolkning være den samme. De engelske versioner af databeskyttelsesdirektivet og databeskyttelsesforordningen støtter dette.

Med kategorier/typer af oplysninger må først og fremmest tænkes på, om der er tale om oplysninger omfattet af artikel 6, 9 eller 10.

I den tilsvarende bestemmelse i persondatalovens § 31, stk. 1, nr. 1, fremgår det, at der skal meddeles indsigt i, *hvilke oplysninger der behandles*. Ordlyden i persondatalovens § 31, stk. 1, må antages at svare både til forordningens krav i artikel 15, stk. 1, litra b, og forord-

ningens krav i artikel 15, stk. 3, 1. pkt., om, at den dataansvarlige udleverer en kopi af de personoplysninger, der behandles.

Der er endvidere den tilføjelse i forordningens artikel 15, stk. 1, litra c, i forhold til ordlyden i persondataloven, at den registrerede også har ret til at få information om de *modtagere*, som personoplysningerne er blevet videregivet til. Efter ordlyden i persondataloven er det kun kategorierne af modtagere af oplysninger, som den registrerede skal oplyses om – men det fremgår klart af forordningens artikel 15, stk. 1, litra c, at indsigtsretten efter denne bestemmelse også vedrører de konkrete modtagere. Det fremgår tilsvarende af databeskyttelsesdirektivets artikel 12, litra a, at den registrerede har ret til at få oplyst modtagerne eller kategorierne af modtagere af oplysningerne. Der er som tidligere anført ikke i persondataloven et krav om, at den registrerede har ret til information om de modtagere, som personoplysningerne er blevet videregivet til, i forbindelse med indsigtsretten. Men der er med databeskyttelsesforordningen herefter ingen tvivl om, at der også skal gives oplysning om modtagere af personoplysninger og ikke kun kategorier af modtagere.

Efter databeskyttelsesforordningens artikel 15, stk. 1, vil den registrerede som efter gældende ret fortsat kun have ret til at få indsigtsret ved den dataansvarlige – hvorfor denne ret fortsat ikke gælder overfor databehandleren.

I gældende ret er der som anført en bestemmelse i persondatalovens § 33, som fastsætter, at den registrerede ikke har krav på en ny meddelelse før 6 måneder efter sidste meddelelse, medmindre der godtgøres en særlig interesse heri.

Databeskyttelsesforordningen har, som anført i afsnit 4.2. om processuelle spørgsmål om de registreredes rettigheder, artikel 12, stk. 3-8, ikke en tilsvarende regel. Databeskyttelsesforordningen viderefører således ikke denne tidsmæssige begrænsning af den registreredes rettighed. I stedet er der et fortolkningsbidrag hertil i præambelbetragtning nr. 63, hvorefter en registreret bør have ret til indsigt i personoplysninger, der er indsamlet om vedkommende, og til let og *med rimelige mellemrum* at udøve denne ret med henblik på at forvisse sig om og kontrollere en behandlings lovlighed.

På baggrund af denne betragtning vil den registrerede, når databeskyttelsesforordningen får virkning, herefter have mulighed for at udøve sin indsigtsret med rimelige mellemrum.

4.5.3.2. Databeskyttelsesforordningens artikel 15, stk. 2 – overførsel til et tredjeland eller en international organisation

Det fremgår af databeskyttelsesforordningens artikel 15, stk. 2, at hvis personoplysningerne overføres til et tredjeland eller en international organisation, har den registrerede ret til

at blive underrettet om de fornødne garantier i medfør af artikel 46 i forbindelse med overførslen.

Det følger allerede af artikel 15, stk. 1, litra c, at den registrerede har ret til indsigt i de modtagere eller kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, navnlig modtagere i tredjelande eller internationale organisationer.

Denne bestemmelse fastsætter, hvad den registrerede yderligere har ret til indsigt i set i forhold til artikel 46 i databeskyttelsesforordningen.

Der er ikke en direkte tilsvarende bestemmelse i persondataloven herom.

For nærmere henvises til afsnit 6.3. om fornødne garantier, artikel 46.

4.5.3.3. Databeskyttelsesforordningens artikel 15, stk. 3 – udlevering af personoplysninger samt formkrav

Det fremgår af databeskyttelsesforordningens artikel 15, stk. 3, at den dataansvarlige udleverer en kopi af de personoplysninger, der behandles. For yderligere kopier, som den registrerede anmoder om, kan den dataansvarlige opkræve et rimeligt gebyr baseret på de administrative omkostninger. Hvis den registrerede indgiver anmodningen elektronisk, og medmindre den registrerede anmoder om andet, udleveres oplysningerne i en almindeligt anvendt elektronisk form.

Meddelelsens form efter databeskyttelsesforordningen ses at svare til, hvad der følger af gældende ret. Derudover fremhæves det, at svaret skal gives elektronisk, såfremt den registrerede har indgivet anmodningen elektronisk, hvilket ses at være et nyt krav i forhold til, hvad der følger af gældende ret.

Det fremgår supplerende af databeskyttelsesforordningens artikel 12, stk. 5, at oplysninger, der gives i henhold til artikel 13 og 14, og enhver meddelelse og enhver foranstaltning, der træffes i henhold til artikel 15-22 og 34, er gratis. Hvis anmodninger fra en registreret er åbenbart grundløse eller overdrevne, især fordi de gentages, kan den dataansvarlige enten: a) opkræve et rimeligt gebyr under hensyntagen til de administrative omkostninger ved at give oplysninger eller meddelelser eller træffe den ønskede foranstaltning, eller b) afvise at efterkomme anmodningen.

Som anført i afsnit 4.2. om processuelle spørgsmål om registreredes rettigheder, artikel 12, stk. 3-8, er der herefter tale om en nyskabelse, hvorefter også en privat – gratis – vil skulle udlevere en kopi af de personoplysninger, der behandles – også selvom oplysninger skal

gives skriftligt. Herefter vil det først være i forbindelse med udlevering af yderligere kopier, som den registrerede anmoder om, være muligt at opkræve et rimeligt gebyr baseret på de administrative omkostninger.

Det fremgår endvidere supplerende af databeskyttelsesforordningens artikel 12, stk. 3, at den dataansvarlige uden unødig forsinkelse og i alle tilfælde senest en måned efter modtagelsen af anmodningen oplyser den registrerede om foranstaltninger, der træffes på baggrund af en anmodning i henhold til artikel 15-22. Denne periode kan forlænges med to måneder, hvis det er nødvendigt, under hensyntagen til anmodningernes kompleksitet og antal. Den dataansvarlige underretter den registrerede om enhver sådan forlængelse senest en måned efter modtagelsen af anmodningen sammen med begrundelsen for forsinkelsen. Hvis den registrerede indgiver en anmodning elektronisk, meddeles oplysningerne så vidt muligt elektronisk, medmindre den registrerede anmoder om andet.

Som en tilføjelse til databeskyttelsesforordningens artikel 15, stk. 3, fremgår det af forordningens artikel 20, stk. 1, om dataportabilitet, at den registrerede har ret til i et struktureret, almindeligt anvendt og maskinlæsbart format at modtage personoplysninger om sig selv, som vedkommende har givet til en dataansvarlig, og har ret til at transmittere disse oplysninger til en anden dataansvarlig uden hindring fra den dataansvarlige, som personoplysningerne er blevet givet til, når: a) behandlingen er baseret på samtykke, jf. artikel 6, stk. 1, litra a, eller artikel 9, stk. 2, litra a, eller på en kontrakt, jf. artikel 6, stk. 1, litra b, og b) behandlingen foretages automatisk.

Det fremgår endvidere af forordningens artikel 20, stk. 2, at når den registrerede udøver sin ret til dataportabilitet i henhold til stk. 1, har den registrerede ret til at få transmitteret personoplysningerne direkte fra en dataansvarlig til en anden, hvis det er teknisk muligt.

4.5.3.4. Databeskyttelsesforordningens artikel 15, stk. 4 – hensynet til andres rettigheder og frihedsrettigheder

Det fremgår af databeskyttelsesforordningens artikel 15, stk. 4, at retten til at modtage en kopi som omhandlet i stk. 3 ikke må krænke andres rettigheder og frihedsrettigheder.

Efter denne bestemmelse vil der derfor skulle ske en afvejning af hensynet til indsigtsretten over for hensynet til andres rettigheder og frihedsrettigheder.

Vedrørende afvejningen følger det af præambelbetragtning nr. 63, at indsigtsretten ikke bør krænke andres rettigheder eller frihedsrettigheder, herunder forretningshemmeligheder eller intellektuel ejendomsret, navnlig den ophavsret, som programmerne er beskyttet af.

Denne vurdering bør dog ikke resultere i en afvisning af at give al information til den registrerede.

Dette stemmer overens med, at der som anført efter gældende ret også vil skulle tages hensyn til private interesser, og herunder menneskerettigheder.

Bestemmelsen i forordningens artikel 15, stk. 4, må således antages at være udtryk for gældende ret – også selvom der ikke er en tilsvarende direkte bestemmelse i persondataloven – idet man også efter gældende ret må skulle tage hensyn til andres rettigheder og frihedsrettigheder i vurderingen af den registreredes indsigtsret.

4.5.4. Overvejelser

Databeskyttelsesforordningens artikel 15, stk. 1, ses overordnet ikke at være en ændring i forhold til gældende ret. Dog er der med artikel 15, stk. 1, litra c, tale om en udvidelse af den dataansvarliges informationspligt til også at informere om modtagere af personoplysninger. Derudover er der tale om en nyskabelse med artikel 15, stk. 1, litra d, e, f og h, som tilføjer de yderligere elementer, der har til formål at oplyse de registrerede om opbevaringsperioden samt retten til berigtigelse, sletning og indgivelse af klager.

Som en nyskabelse i forhold til persondataloven fastsætter databeskyttelsesforordningens artikel 15, stk. 2, at hvis personoplysningerne overføres til et tredjeland eller en international organisation, har den registrerede ret til at blive underrettet om de fornødne garantier i medfør af artikel 46 i forbindelse med overførslen.

Forordningens artikel 15, stk. 3, fastsætter kravene til formen af den meddelelse, som følger af indsigtsretten. Efter databeskyttelsesforordningen ses formen heraf at svare til, hvad der følger af gældende ret – dog fremhæves det, at svaret skal gives elektronisk, såfremt den registrerede har anmodet elektronisk, hvilket ses at være et nyt krav i forhold til, hvad der følger af gældende ret.

Bestemmelsen i forordningens artikel 15, stk. 4, antages at være udtryk for gældende ret – også selvom der ikke er en tilsvarende direkte bestemmelse i persondataloven – idet man også efter gældende ret må skulle tage hensyn til andres rettigheder og frihedsrettigheder i vurderingen af den registreredes indsigtsret.

Det bemærkes, at undtagelserne til den registreredes indsigtsret i persondatalovens § 32 ikke er videreført i databeskyttelsesforordningen. For nærmere om forordningens mulighed for begrænsning i indsigtsretten henvises til afsnit 4.13. om begrænsninger af rettighederne, artikel 23.

4.6. Berigtigelse, artikel 16

4.6.1. Præsentation

Persondatalovens § 37, stk. 1, fastsætter, at den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Databeskyttelsesdirektivets artikel 12, litra b, og persondatalovens § 37, stk. 1, regulerer i én og samme bestemmelse ret til sletning, berigtigelse og blokering af oplysninger, mens forordningens artikel 16 regulerer ret til berigtigelse, artikel 17 regulerer ret til sletning og artikel 18 regulerer ret til begrænsning af behandling.

Databeskyttelsesforordningens artikel 16 fastsætter, at den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. Den registrerede har under hensyntagen til formålene med behandlingen, ret til få fuldstændiggjort ufuldstændige personoplysninger, bl.a. ved at fremlægge en supplerende erklæring.

4.6.2. Gældende ret

Det fremgår af persondatalovens § 37, stk. 1, at den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Bestemmelsen er baseret på artikel 12, litra b, i databeskyttelsesdirektivet, hvoraf det fremgår, at medlemsstaterne sikrer enhver registreret ret til hos den dataansvarlige efter omstændighederne at få oplysninger, som ikke er blevet behandlet i overensstemmelse med dette direktiv, berigtiget, slettet eller blokeret, navnlig hvis de er ufuldstændige eller urigtige.

Det fremgår af bemærkningerne til persondatalovens § 37, stk. 1, at en anmodning om berigtigelse, sletning eller blokering skal komme fra den registrerede eller dennes fuldmægtig. Anmodningen skal angå oplysninger om den registrerede selv. Den dataansvarlige er således ikke forpligtet til efter anmodning at foretage berigtigelse mv. af oplysninger om andre personer. Dog vil det efter omstændighederne påhvile den dataansvarlige at undersø-

ge rigtigheden af sådanne henvendelser, jf. persondatalovens § 5, stk. 4.[397] For så vidt angår offentlige myndigheder kan det imidlertid følge af begrebet god forvaltningsskik, at myndigheden er forpligtet til efter anmodning at foretage berigtigelse af oplysninger om andre personer.[398]

Det fremgår endvidere af bemærkningerne til persondataloven, at der ikke gælder noget formkrav til den registreredes anmodninger i henhold til bestemmelsen. Hvis anmodning fremsættes, påhviler det den dataansvarlige eller dennes repræsentant snarest muligt at tage stilling til, om begæringen kan imødekommes, og i givet fald at foretage berigtigelse, sletning eller blokering.[399]

Det fremgår endelig af bemærkningerne til persondataloven, at om oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lovgivningen, skal berigtiges, slettes eller blokeres, må afgøres ud fra de konkrete omstændigheder.[400] Datatilsynet anfører tilsvarende, at hvorvidt der skal foretages sletning, berigtigelse eller blokering, som udgangspunkt afgøres af den dataansvarlige ud fra de konkrete omstændigheder.[401] Det fremgår desuden af bemærkningerne til persondataloven, at i enkelte situationer kan det dog følge af bl.a. lovgivningen, at en bestemt korrigeringsmetode under nærmere angivne omstændigheder skal anvendes. Dette er eksempelvis tilfældet for så vidt angår reglen i retsplejelovens § 221 om, i hvilket omfang domstolene kan berigtige afgørelser. Det forudsættes, at sådanne særlige regler går forud for persondatalovens § 37. Der gælder således ikke en pligt til at foretage berigtigelse, sletning eller blokering i de tilfælde, hvor andet – ud fra særlige hensyn – er fastsat i lovgivningen i øvrigt. Det bemærkes, at en sådan ordning er forenelig med direktivets artikel 12, litra b, jf. herved udtrykket »efter omstændighederne«.[402]

Datatilsynet har udfærdiget en pjece; "Kend din ret. Når du mener, der er forkerte oplysninger i myndigheders sager", som omhandler berigtigelse af urigtige oplysninger om en person, som behandles i den offentlige forvaltnings digitale sager, og hvoraf det følger, at

[397] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[398] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.3.1.
[399] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[400] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[401] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.3.1.
[402] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.

der gælder særlige forhold ved myndigheders registrering af – og eventuelle senere ændring af – oplysninger.

Det fremgår således af pjecen, at i den situation, hvor der er *uenighed* mellem den dataansvarlige og den registrerede omkring oplysningernes rigtighed – og det ikke med sikkerhed kan fastslås, hvem der har ret – skal myndigheden sørge for, at der bliver lavet en tilføjelse til oplysningerne, hvoraf det skal fremgå, at der er uenighed om oplysningernes rigtighed.[403]

Det følger derudover af pjecen, at i den situation, hvor der er enighed mellem den dataansvarlige og den registrerede om oplysningernes rigtighed, vil myndigheden ikke altid kunne slette de bestridte oplysninger. I den situation vil myndigheden ofte foretage en berigtigelse af oplysningerne ved at skrive, at de oprindeligt noterede oplysninger er forkerte.[404]

Endvidere anfører Datatilsynet i pjecen, at myndigheder ofte skriver deres vurdering af forskellige spørgsmål, eksempelvis en læges eller en socialrådgivers faglige vurdering af et forhold. I disse situationer, vil det normalt ikke være muligt for Datatilsynet at fastslå, om den faglige vurdering er korrekt, hvorfor det ikke kan statueres, at oplysningerne er urigtige eller vildledende. Også i sådanne situationer vil myndigheden skulle tilføje oplysninger om den registreredes synspunkter. Dette eksemplificeres i et eksempel, hvor en skoleleder skriver til en kommune, at han er bekymret for, om der er misbrug i den registreredes hjem. Den registrerede kan så få tilføjet, at personen er uenig i, at der er misbrug. Men den registrerede kan ikke få slettet skolelederens indberetning.[405]

Datatilsynet har i sin årsberetning 2011 udtalt, at det var tilsynets opfattelse, at tilsynet efter persondatalovens § 37 ikke havde mulighed for at efterprøve udlændingemyndighedernes afgørelser om fastlæggelse af klagernes fødselsdato og fødselssted. Persondatalovens § 37 tilsigter efter Datatilsynets opfattelse ikke at give tilsynet kompetence til at vurdere indholdsmæssige spørgsmål, der er reguleret af anden lovgivning som eksempelvis udlændingelovgivningen.[406]

Det antages, at der vil skulle meget til, for at en registreret person efter persondatalovens § 37, stk. 1, kan kræve korrektion af selve de oplysninger, som afspejler den dataansvarliges

[403] Datatilsynets pjece "Kend din ret. Når du mener, der er forkerte oplysninger i myndigheders sager".
[404] Datatilsynets pjece "Kend din ret. Når du mener, der er forkerte oplysninger i myndigheders sager".
[405] Datatilsynets pjece "Kend din ret. Når du mener, der er forkerte oplysninger i myndigheders sager".
[406] Datatilsynets årsberetning 2011, s. 26.

subjektive vurdering af et sagsforhold, herunder eksempelvis den dataansvarliges subjektive vurdering af, hvad der er blevet sagt på et møde med den registrerede eller lignende.[407]

Fra praksis kan derudover nævnes en sag vedrørende spørgsmål om berigtigelse af journaloplysninger, hvor Datatilsynet ikke fandt, at der var grundlag for i medfør af persondatalovens § 37 eller § 5 at pålægge Indenrigs- og Sundhedsministeriet at foretage berigtigelse i journalsystemet vedrørende den registrerede. Datatilsynet fandt ikke, at det forhold, at en myndighed valgte at anvende en anden journaliseringstekst, end den registrerede ønskede, kunne føre til, at der kunne kræves berigtigelse efter persondatalovens bestemmelser, når der i øvrigt ikke vurderedes at være tale om urigtige eller vildledende oplysninger. Datatilsynet lagde herved vægt på, at journalsystemet er et arbejdsredskab, der først og fremmest skal sikre identificering og genfinding af de dokumenter, som myndigheden modtager og producerer, og at der derfor som oftest anvendes korte og standardiserede journaliseringstekster. På baggrund af de foreliggende oplysninger fandt Datatilsynet det ikke sandsynliggjort, at der blev behandlet urigtige eller vildledende oplysninger i Indenrigs- og Sundhedsministeriets journalsystem.[408]

4.6.3. Databeskyttelsesforordningen

Det fremgår af Kommissionens forslag til databeskyttelsesforordningen, at i artikel 16 fastsættes den registreredes ret til berigtigelse, som er baseret på artikel 12, litra b, i databeskyttelsesdirektivet.[409]

Det fremgår af databeskyttelsesforordningens artikel 16, at den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. Den registrerede har under hensyntagen til formålene med behandlingen ret til få fuldstændiggjort ufuldstændige personoplysninger, bl.a. ved at fremlægge en supplerende erklæring.

Derudover fremgår der af databeskyttelsesforordningens artikel 5, stk. 1, litra d, et princip om, at personoplysninger skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«).

Det fremgår endvidere af præambelbetragtning nr. 39, at der bør træffes enhver rimelig foranstaltning for at sikre, at personoplysninger, som er urigtige, berigtiges eller slettes.

[407] Persondataloven med kommentarer (2015), s. 532.
[408] Sag vedrørende spørgsmål om berigtigelse af journaloplysninger, Datatilsynets j.nr. 2003-311-0273.
[409] Se Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig).

Det fremgår endelig af præambelbetragtning nr. 65, at en registreret bør have ret til at få berigtiget sine personoplysninger og »ret til at blive glemt«, hvis opbevaringen af sådanne oplysninger overtræder denne forordning eller EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt.

For så vidt angår ordlyden i forordningens artikel 16, i forhold til persondatalovens § 37, stk. 1, og databeskyttelsesdirektivets artikel 12, litra b, ses indholdet på baggrund af en ordlydsfortolkning stort set at være identisk.

Som udgangspunkt vil forordningens artikel 16 derfor have samme anvendelsesområde som gældende ret. Der er dog nogle forskelle i bestemmelsernes udformning, som det er relevant at vurdere.

Efter persondatalovens § 37, stk. 1, vil den dataansvarlige, som udgangspunkt kunne vælge mellem, hvilken korrigeringsmetode, der skal benyttes i forbindelse med urigtige oplysninger. Den dataansvarlige kan således vælge mellem enten berigtigelse, sletning eller blokering. I databeskyttelsesforordningen er den bestemmelse, som svarer nogenlunde til persondatalovens § 37, stk. 1, opdelt i 3 selvstændige artikler – henholdsvis forordningens artikel 16, 17 og 18.

At der således er sket en opdeling af bestemmelsen i tre selvstændige artikler taler for, at den registrerede netop har ret til at vælge eksempelvis berigtigelse, jf. artikel 16 (dog under forudsætning af, at betingelserne i artiklerne er opfyldt). Såfremt den registreredes henvender sig til den dataansvarlige og ønsker urigtige personoplysninger berigtiget, må det efter databeskyttelsesforordningen antages, at den dataansvarlige vil skulle berigtige disse. Der er formentlig ikke tale om en situation, der vil få større praktisk betydning, idet en registreret for det meste må antages at ville være ligeså interesseret i at få urigtige oplysninger slettet, som i at få dem berigtiget.

Det fremgår, som anført af bemærkningerne til persondatalovens § 37, stk. 1, at berigtigelsen skal ske *snarest muligt*. Efter databeskyttelsesforordningens artikel 16 fremgår det, at berigtigelsen skal ske *uden unødig forsinkelse*. På baggrund af en ordlydsfortolkning af snarest muligt og uden unødig forsinkelse ses den indholdsmæssige betydning af ordene at være den samme. Efter en samlet vurdering må hastigheden af, hvornår der skal ske berigtigelse af urigtige personoplysninger efter databeskyttelsesforordningen, derfor skulle forstås i overensstemmelse med gældende ret.

I databeskyttelsesforordningens artikel 16 er der en yderligere tilføjelse til den registreredes ret til berigtigelse, som fastslår, at den registrerede, under hensyntagen til formålene

med behandlingen, har ret til at få fuldstændiggjort ufuldstændige personoplysninger, bl.a. ved at fremlægge en supplerende erklæring. Denne ret til at fremlægge en erklæring følger ikke direkte af gældende ret, men det må også efter gældende ret antages, at den registrerede kan have en ret til at fremlægge en supplerende erklæring. Under alle omstændigheder vil den registrerede i hvert fald efter databeskyttelsesforordningen, have ret til at fremlægge en sådan supplerende erklæring.

Overordnet ses forordningens artikel 16 således at være i overensstemmelse med gældende ret – dog vil den registrerede som noget nyt kunne vælge, om oplysninger skal berigtiges eller slettes inden for rammerne af artikel 16 og 17, ligesom databeskyttelsesforordningen indeholder en tilføjelse om, at den registrerede har ret til af få fuldstændiggjort ufuldstændige personoplysninger, bl.a. ved at fremlægge en supplerende erklæring.

4.6.4. Overvejelser

Databeskyttelsesforordningens artikel 16 er udtryk for en videreførelse af gældende ret – dog vil den registrerede kunne vælge, om oplysninger skal berigtiges eller slettes inden for rammerne af artikel 16 og 17, ligesom databeskyttelsesforordningen indeholder en tilføjelse om, at den registrerede har ret til af få fuldstændiggjort ufuldstændige personoplysninger, bl.a. ved at fremlægge en supplerende erklæring.

4.7. Ret til sletning ("retten til at blive glemt"), artikel 17

4.7.1. Præsentation

Forordningens artikel 17 omhandler den registreredes ret til at få personoplysninger om sig selv slettet. Stk. 1 omhandler de situationer, hvor den dataansvarlige har *pligt* til at *slette* personoplysninger. Stk. 2 omhandler den dataansvarliges forpligtelse til underretning af andre dataansvarlige i tilfælde af, at den dataansvarlige har *offentliggjort* personoplysninger, som den dataansvarlige er forpligtet til at slette. Stk. 3 indeholder *undtagelser* til bestemmelserne i stk. 1 og 2.

4.7.2. Gældende ret

Det følger af persondatalovens § 37, stk. 1, at den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom. Bestemmelsen er baseret på artikel 12, litra b, i databeskyttelsesdirektivet, hvoraf det fremgår, at medlemsstaterne sikrer enhver registreret ret til hos den dataansvarlige efter omstændighederne at få oplysninger, som ikke er behandlet i

overensstemmelse med databeskyttelsesdirektivet, berigtiget, slettet eller blokeret, navnlig hvis de er ufuldstændige eller urigtige.

Det fremgår af bemærkningerne til persondatalovens § 37, stk. 1, at det må afgøres ud fra de konkrete omstændigheder, om oplysninger, der viser sig urigtige, vildledende eller på lignede måder behandlet i strid med lovgivningen, skal slettes, berigtiges eller blokeres. Særlige regler om, at en bestemt korrigeringsmetode skal anvendes, går forud for bestemmelsen i § 37, stk. 1.[410] Der gælder således ikke en pligt til at foretage berigtigelse, sletning eller blokering i de tilfælde, hvor andet – ud fra særlige hensyn – er fastsat i lovgivningen i øvrigt.

Det fremgår desuden af bemærkningerne til persondatalovens § 37, stk. 1, at en anmodning om berigtigelse, sletning eller blokering skal komme fra den registrerede selv eller dennes fuldmægtig.[411] Anmodningen skal angå oplysninger om den registrerede selv. Den dataansvarlige er ikke forpligtet til at foretage berigtigelse mv. af oplysninger om andre personer. Dog vil der efter omstændighederne påhvile den dataansvarlige en forpligtelse til at undersøge rigtigheden af sådanne henvendelser, jf. persondatalovens § 5, stk. 4. Det fremgår i øvrigt, at der ikke gælder noget formkrav til den registreredes anmodning.

Det fremgår af persondataloven med kommentarer, at det må antages, at der vil skulle meget til (i form af et meget sikkert grundlag), for at en registreret person efter § 37, stk. 1, kan kræve korrektion af selve de oplysninger, som afspejler den dataansvarliges (egen) subjektive vurdering af et sagsforhold.[412] I sådanne tilfælde, hvor det ikke kan fastslås, at der behandles urigtige eller vildledende oplysninger, vil det i stedet – alt efter indsigelsens karakter – kunne følge af kravet om god databehandlingsskik, jf. persondatalovens § 5, stk. 1, at den dataansvarlige skal sørge for, at den registrerede persons indsigelse mod de behandlede oplysninger kommer til at fremgå af sagen.

Det fremgår desuden af persondataloven med kommentarer, at det i praksis ofte vil være sådan, at reglen i § 37 (lige som § 5, stk. 4) ikke fører til, at oplysninger der viser sig urigtige, skal slettes.[413] Dette gælder, uanset om oplysningerne har været urigtige siden indsamlingen, eller de først er blevet det senere, fordi forholdene har ændret sig. Denne manglende pligt for offentlige myndigheder til at slette oplysninger skyldes bl.a. journaliseringspligten i offentlighedslovens § 15. Når offentlige myndigheder skal berigtige urigtige

[410] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[411] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[412] Persondataloven med kommentarer (2015), s. 532.
[413] Persondataloven med kommentarer (2015), s. 534 f.

eller vildledende oplysninger, vil det derfor ofte skulle ske ved at notere berigtigelsen (de korrekte oplysninger) på sagen uden at fjerne de oplysninger, der i forvejen fremgik. Det kan eventuelt ske i form af et notat, der lægges på sagen. Dette krav beskrives nærmere i et svar af 30. juni 1998 på et § 20-spørgsmål afgivet af justitsministeren, hvoraf det fremgår, at en myndighed i almindelighed ikke er berettiget til at fjerne/destruere bestemte dokumenter, der indgår i en sag. Det kan normalt kun ske, hvis der er lovhjemmel hertil. Dette er bl.a. begrundet i hensynet til, at myndigheden senere – f.eks. i forbindelse med klager eller genoptagelse – skal kunne dokumentere, hvad der er passeret i en sag.[414]

Det følger af persondatalovens § 37, stk. 2, at den dataansvarlige skal underrette den tredjemand, hvortil oplysningerne er videregivet, om, at de videregivne oplysninger er berigtiget, slettet eller blokeret i henhold til § 37, stk. 1, hvis en registreret fremsætter anmodning herom. Dette gælder dog ikke, hvis underretningen viser sig umulig eller uforholdsmæssig vanskelig. Det er i den forbindelse vigtigt at være opmærksom på, at persondatalovens § 37, stk. 2, kun finder anvendelse i de situationer, hvor det er blevet fastslået, at f.eks. en myndighed behandler urigtige eller vildledende oplysninger.

Det fremgår af bemærkningerne til bestemmelsen, at det, hvis anmodning fremsættes, påhviler den dataansvarlige eller dennes repræsentant snarest muligt at tage stilling til, om begæringen kan imødekommes, og i givet fald at underrette de tredjemænd, hvortil oplysningerne om den registrerede er videregivet.[415] Der gælder ikke formkrav til underretningen, men det skal i underretningen angives, hvilken korrigeringsmetode der er anvendt. Heri ligger der ifølge bemærkningerne til bestemmelsen, at der skal gives tredjemand underretning om anledningen til, at berigtigelse, sletning eller blokering har fundet sted.[416]

For så vidt angår spørgsmålet om, hvornår noget er uforholdsmæssigt vanskeligt, fremgår det af persondataloven med kommentarer, at dette vil bero på en afvejning af på den ene side betydningen af underretningen for den registrerede og på den anden side den arbejdsindsats hos den dataansvarlige, som vil være forbundet med en underretning. Der skal foretages en afvejning i hvert enkelt tilfælde af alle de momenter, som kan tillægges vægt i vurderingen af de nævnte modsatrettede hensyn. Det fremgår desuden, at det under hensyntagen til at den registrerede selv skal anmode om, at der gives underretning til de tredjemænd, som har modtaget urigtige eller vildledende oplysninger om vedkommende i almindelighed vil skulle lægges til grund, at det er af stor betydning for den registrerede at

[414] Svar på spørgsmål nr. S 580 af 30. juni 1998.
[415] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[416] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.

en sådan underretning gives.[417] Det fremgår videre, at det oftest ikke vil være forbundet med store arbejdsmæssige eller ressourcemæssige belastninger for den dataansvarlige at foretage underretning, hvorfor underretning som hovedregel skal gives, og at der skal anføres tungtvejende argumenter for, at den dataansvarlige kan undlade at give underretning.[418]

EU-Domstolens dom af 13. maj 2014 i Google-sagen (sag C-131/12) omhandlede "*retten til at blive glemt*" på internettet. Domstolen fastslog heri for det første, at artikel 12, litra b, og artikel 14, stk. 1, litra a, i databeskyttelsesdirektivet skal fortolkes således, at en søgemaskineudbyder med henblik på at overholde de rettigheder, der er fastsat i de pågældende bestemmelser, og for så vidt som de betingelser, der er fastsat i direktivet, faktisk er opfyldt, er forpligtet til fra den resultatliste, der vises efter en søgning på en persons navn, at fjerne link til hjemmesider, som er offentliggjort af tredjemand og indeholder oplysninger vedrørende denne person, også i det tilfælde, hvor dette navn eller disse oplysninger ikke forudgående eller samtidig slettes fra disse hjemmesider, og i givet fald selv når offentliggørelsen på disse sider i sig selv er lovlig.

Ansvaret for at fjerne links til hjemmesider, der indeholder oplysninger om en fysisk person, er med andre ord søgemaskineudbyderens – og ikke hjemmesideudbyderens, jf. navnlig dommens præmis 80-82.

Det følger i øvrigt af dommens præmisser, at den ret til at blive glemt, som ifølge EU-Domstolen følger af databeskyttelsesdirektivet, ikke er absolut. Der vil således skulle foretages en vurdering i den enkelte sag af, om en registreret person kan gøre krav på at få fjernet links til hjemmesider fra en resultatliste på en søgemaskine, idet der ifølge dommen skal lægges vægt på, at hensynet til beskyttelse af personlige oplysninger som udgangspunkt vil overstige de modstående hensyn til offentlighed omkring oplysningerne, og at det kun vil være i særlige situationer, at indgreb i den grundlæggende rettighed til at blive glemt, vil kunne retfærdiggøres.

Som det i forlængelse heraf fremgår af persondataloven med kommentarer, skal bestemmelserne i persondatalovens §§ 35 og 37, stk. 1, anvendes i overensstemmelse hermed.[419]

Det følger af persondatalovens § 38, at den registrerede kan tilbagekalde et samtykke. Det fremgår af bemærkningerne til persondatalovens § 38, at den registrerede på et hvilket som helst tidspunkt kan tilbagekalde sit samtykke. Det fremgår desuden, at et samtykke ikke

[417] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[418] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[419] Persondataloven med kommentarer (2015), s. 538.

kan tilbagekaldes med "tilbagevirkende kraft", og at virkningen af en tilbagekaldelse er, at den behandling af oplysninger, som den registrerede har meddelt sit samtykke til, normalt ikke må finde sted fremover. Det fremgår desuden, at det må afgøres ud fra en konkret vurdering, om oplysningerne i så fald skal slettes eller blokeres.[420]

4.7.3. Databeskyttelsesforordningen

Det fremgår af Kommissionens forslag til databeskyttelsesforordning, at artikel 17 uddyber og beskriver retten til sletning, der er omhandlet i databeskyttelsesdirektivets artikel 12, litra b, og angiver betingelserne for retten til at blive glemt, herunder den pligt, som dataansvarlige, der har offentliggjort personoplysninger, har til at informere tredjeparter om den registreredes anmodning om at slette alle link til, kopier eller gengivelser af de pågældende personoplysninger.

4.7.3.1. Ret til sletning – artikel 17, stk. 1

Det fremgår af bestemmelsen i forordningens artikel 17, stk. 1, hvornår en registreret har ret til at få personoplysninger om sig slettet af den dataansvarlige uden unødig forsinkelse, og den dataansvarlige samtidig har pligt til at slette personoplysninger uden unødig forsinkelse.

Bestemmelsen i artikel 17, stk. 1, må skulle forstås således, at forpligtelsen for den dataansvarlige til at slette som udgangspunkt alene opstår, når den registrerede gør brug af sin ret.

Dette ændrer dog ikke på, at den dataansvarlige til stadighed skal overholde principperne i artikel 5 om bl.a. formålsbegrænsning, dataminimering, rigtighed og opbevaringsbegrænsning.

Bestemmelsen gælder for enhver, men i præambelbetragtning nr. 65 fremhæves, at retten navnlig er relevant, når den registrerede har givet sit samtykke som barn og ikke fuldt ud var bekendt med risiciene i forbindelse med behandling, og senere ønsker at fjerne sådanne oplysninger, særligt på internettet. Det fremgår desuden, at den registrerede bør kunne udøve denne rettighed, uanset om vedkommende ikke længere er barn.

Den registreredes ret til sletning, og den dataansvarliges dertil hørende forpligtelse til at slette, opstår i medfør af artikel 17, stk. 1, når ét af følgende forhold gør sig gældende:

a) Personoplysningerne er ikke længere nødvendige til at opfylde de formål, hvortil de blev indsamlet eller på anden vis behandlet.

[420] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 38.

b) Den registrerede trækker det samtykke, der er grundlaget for behandlingen, jf. artikel 6, stk. 1, litra a, eller artikel 9, stk. 2, litra a, tilbage, og der er ikke et andet retsgrundlag for behandlingen.
c) Den registrerede gør indsigelse mod behandlingen i henhold til artikel 21, stk. 1, og der foreligger ikke legitime grunde til behandlingen, som går forud for indsigelsen, eller den registrerede gør indsigelse mod behandlingen i medfør af artikel 21, stk. 2.
d) Personoplysningerne er blevet behandlet ulovligt.
e) Personoplysningerne skal slettes for at overholde en retlig forpligtelse i EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt.
f) Personoplysningerne er blevet indsamlet i forbindelse med udbud af informationssamfundstjenester som omhandlet i artikel 8, stk. 1.

For så vidt angår litra a, svarer bestemmelsens ordlyd til ordlyden i persondatalovens § 5, stk. 5. Bestemmelsen må antages at få selvstændigt indhold i forhold til artikel 5, stk. 1, litra e, i de tilfælde, hvor den registrerede gør brug af sin ret til sletning *uden unødig forsinkelse* i tilfælde, hvor den dataansvarlige ellers kunne afvente f.eks. udløbet af en generelt fastsat slettefrist.

Bestemmelsen i litra b må antages at svare til persondatalovens § 38 om tilbagekaldelse af samtykke.

Vedrørende forpligtelsen i litra c henvises der til afsnit 4.11. om artikel 21 og indsigelsesretten.

Bestemmelsen i litra d skal ses i sammenhæng med forordningens artikel 5 om principper for behandling af personoplysninger, og det må antages, at forpligtelsen til at slette oplysningerne i medfør af litra d som udgangspunkt vil gælde for den dataansvarlige, uanset om den registrerede gør brug af sin rettighed i henhold til bestemmelsen, og eventuelt kan den dataansvarlige være forpligtet til at slette *straks* i medfør af bestemmelsen i artikel 5, stk. 1, litra d.

Det samme må antages at gøre sig gældende i forhold til sletning i de situationer, som er omhandlet i litra e, dog kan fristen i artikel 17 (uden unødig forsinkelse) give bestemmelsen et selvstændigt indhold.

Litra f må antages at supplere litra b i de tilfælde, hvor forældremyndighedsindehaveren har givet samtykke på vegne af en registreret, som på tidspunktet for registreringen var et barn under 16, og den registrerede nu, uanset om vedkommende ikke længere er et barn, jf. herved præambelbetragtning nr. 65, ønsker at gøre brug af retten til sletning.

4.7.3.2. Underretningspligt – artikel 17, stk. 2

Ifølge artikel 17, stk. 2, skal den dataansvarlige, hvis denne har offentliggjort personoplysninger og i henhold til stk. 1 er forpligtet til at slette de pågældende oplysninger, under hensyntagen til den teknologi, der er tilgængelig, og omkostningerne ved implementeringen, træffe rimelige foranstaltninger, herunder tekniske foranstaltninger, for at underrette de dataansvarlige, som behandler de pågældende personoplysninger, om, at den registrerede har anmodet *disse dataansvarlige* om at slette *alle link til eller kopier eller gengivelser* af de pågældende personoplysninger.

Det fremgår af præambelbetragtning nr. 66, at for at styrke retten til at blive glemt i onlinemiljøet bør retten til sletning udvides, så en dataansvarlig, der har offentliggjort personoplysninger, forpligtes til at underrette de dataansvarlige, der behandler sådanne personoplysninger, med henblik på at få slettet alle link til, kopier eller gengivelser af disse personoplysninger. I den forbindelse bør den dataansvarlige tage rimelige skridt under hensyntagen til den tilgængelige teknologi og de midler, som den dataansvarlige har til sin rådighed, herunder tekniske foranstaltninger, til at informere de dataansvarlige, der behandler personoplysningerne, om den registreredes anmodning.

Bestemmelsen forpligter alene *dataansvarlige*, og ikke databehandlere, og forpligtelsen angår alene oplysninger, som den dataansvarlige har *offentliggjort*.

Selve underretningen skal indeholde oplysninger om, at den registrerede har anmodet de dataansvarlige, som behandler de pågældende personoplysninger, om at slette alle link til eller kopier eller gengivelser af de pågældende personoplysninger.

Spørgsmålet om, hvilke *rimelige* foranstaltninger den dataansvarlige, som har offentliggjort de pågældende personoplysninger, som nu skal slettes, skal træffe, for at underrette andre dataansvarlige, skal ifølge bestemmelsens ordlyd afgøres konkret under hensyntagen til den teknologi, der er tilgængelig, og omkostningerne ved implementeringen af de foranstaltninger, som skal til for at foretage en sådan underretning.

Det fremgår ikke af bestemmelsen, *hvornår* den dataansvarlige skal foretage underretning. Det må dog antages at skulle ske inden for rimelig tid, ligesom det i øvrigt må antages, at der vil kunne være tilfælde, hvor en dataansvarlig, som på sletningstidspunktet ikke var forpligtet til at underrette, alligevel bliver forpligtet til at foretage underretning på et senere tidspunkt, f.eks. hvis den teknologiske udvikling har gjort underretning i det konkrete tilfælde enkel og mulig uden høje omkostninger.

En dataansvarlig, som *modtager underretningen*, bliver – ud fra bestemmelsens ordlyd i artikel 17, stk. 2 – ikke *direkte* forpligtet til at slette de pågældende oplysninger, men det må antages, at en sådan dataansvarlig i lyset af underretningen må vurdere, om oplysningerne skal slettes hos den pågældende dataansvarlige, jf. principperne i artikel 5, stk. 1, litra e, og artikel 17, stk. 1.

Som det fremgår af præambelbetragtning nr. 66 er der tale om en *udvidelse* af retten til sletning i tilfælde, hvor en dataansvarlig har offentliggjort personoplysninger.

Underretningsforpligtelsen i artikel 17, stk. 2, suppleres af artikel 19, hvorefter den dataansvarlige har underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling, medmindre dette viser sig umuligt eller uforholdsmæssigt vanskeligt.

4.7.3.3. Undtagelser – artikel 17, stk. 3

I artikel 17, stk. 3, er der fastsat en række undtagelser fra den registreredes ret til sletning og den dataansvarliges pligt til at foretage sletning uden unødig forsinkelse, og fra den dataansvarliges pligt til underretning, og dermed fra "retten til at blive glemt".

Oplysninger kan i medfør af litra a bevares i det omfang, behandlingen er nødvendig for at udøve retten til ytrings- og informationsfrihed. Der henvises til afsnit 10.1. om artikel 85 om behandling og ytrings- og informationsfriheden.

Oplysninger kan i medfør af litra b bevares i det omfang, det er nødvendigt for at overholde en retlig forpligtelse, der kræver behandling i henhold til EU-retten eller medlemsstaternes nationale ret, og som den dataansvarlige er underlagt, eller for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Det må på den baggrund antages, at artikel 17 ikke indeholder en selvstændig ret til at blive glemt i den offentlige sektor. Dette skyldes, at det ofte vil være nødvendigt for offentlige myndigheder at kunne dokumentere det grundlag, som en afgørelse eller anden beslutning i sin tid blev truffet på. Især offentlige myndigheder bør udvise en betydelig tilbageholdenhed med helt at slette oplysningerne, som på et tidspunkt har udgjort en del af det grundlag, som en afgørelse er truffet på. Når offentlige myndigheder skal slette urigtige eller vildledende oplysninger, vil det derfor ofte skulle ske ved at notere berigtigelsen (de korrekte oplysninger) på sagen uden at fjerne de oplysninger, der i forvejen fremgik. Det kan eventuelt ske i form af et notat, der lægges på sagen.

En egentlig sletning vil oftere kunne kræves, hvis der er tale om oplysninger, som eksempelvis indgår i et register eller andet informationssystem, hvorfra oplysningerne tilgår andre dataansvarlige. Det må imidlertid også her efter omstændighederne accepteres, at det gennem en fortsat opbevaring af en kopi af registeret i dets tidligere version eller på anden måde kan dokumenteres, hvilke oplysninger, der tidligere måtte være blevet videregivet.

Der bemærkes endvidere, at en fortsat opbevaring på arkiv under alle omstændigheder vil kunne komme på tale. Der henvises til afsnit 10.6. om rammerne i artikel 89, stk. 1 og 3 samt 4, vedrørende arkivformål i samfundets interesse.

Det følger af litra c, at oplysninger kan bevares i det omfang, behandlingen er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet. Der henvises til afsnit 3.7.-3.9. om artikel 9.

Det følger af litra d, at oplysninger kan bevares i det omfang, behandlingen er nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål. Der henvises til afsnit 10.5.-10.6., om artikel 89.

Det følger endelig af litra e, at oplysninger kan bevares i det omfang, det er nødvendigt for, at retskrav kan fastlægges, gøres gældende eller forsvares.

Der er med artikel 17, stk. 3, alt i alt tale om meget betydelige undtagelser. Det må på den baggrund antages, at der alene vil være et begrænset rum for den registrerede til at udnytte retten til at blive glemt i den offentlige sektor.

4.7.4. Overvejelser

På baggrund af de omfattende undtagelser til retten til sletning og "retten til at blive glemt" og fortolkningsbidraget i forordningsforslaget om, at artikel 17 uddyber og beskriver retten til sletning, må det antages, at forordningens artikel 17 overordnet set er en videreførelse af gældende ret.

4.8. Ret til begrænsning af behandling, artikel 18

4.8.1. Præsentation

Forordningens artikel 18 fastsætter nærmere regler om, hvornår den registrerede har ret til at få begrænset behandlingen af personoplysninger, herunder nærmere regler om, hvad begrænsning af behandling indebærer.

4.8.2. Gældende ret

Der henvises til omtalen af persondatalovens § 37 i afsnit 4.7. om forordningens artikel 17.

Databeskyttelsesdirektivets artikel 12, litra b, og persondatalovens § 37 regulerer ret til sletning, berigtigelse og blokering af oplysninger, mens forordningens artikel 16 regulerer ret til berigtigelse, artikel 17 regulerer ret til sletning og artikel 18 regulerer ret til begrænsning af behandling.

Det fremgår af bemærkningerne til persondatalovens § 37, at korrigeringsmetoden *blokering* er udtryk for en nyskabelse. Blokering af oplysninger indebærer, at det fortsat er tilladt at opbevare indsamlede oplysninger, hvorimod det ikke er tilladt i øvrigt at behandle og bruge oplysninger, herunder navnlig videregive dem til tredjemand. Oplysninger, som er blokeret, skal derfor være forsynet med en sådan markering, at en bruger informeres om blokeringen. Det forhold, at behandlede oplysninger er blokeret, er ikke til hinder for, at den dataansvarlige foretager den behandling, som er nødvendig for, at den dataansvarlige kan opfylde en oplysningspligt, som påhviler denne, f.eks. efter lovgivningen. Således vil en forvaltningsmyndighed i medfør af reglerne i forvaltningsloven og offentlighedsloven om aktindsigt kunne meddele tredjemand aktindsigt i de blokerede oplysninger. I givet fald forudsættes det, at tredjemand informeres om, at der er tale om oplysninger, som er blokeret, og om, hvorfor dette er sket.[421]

Begrebet blokering er hentet fra tysk ret, hvor blokering indebærer "en markering af lagrede oplysninger med henblik på at begrænse yderligere behandling eller brug af disse". Dette er oplyst af den føderale tyske tilsynsmyndighed i en skrivelse til Registertilsynet. Det må antages, at der i visse situationer, som en mindre vidtgående foranstaltning, vil kunne træffes afgørelse om *begrænset blokering*, således at behandling af de pågældende oplysninger ikke kan omfatte bestemte typer af behandling, f.eks. videregivelse eller behandling til bestemte formål, f.eks. markedsføring.[422]

Højesteret tog i U 2007.2331/1 H stilling til, om en advokat, A, under en tvangsfjernelsessag måtte fremlægge 2 bilag, til trods for, at kommunen, K, havde meddelt hende, at den i henhold til persondatalovens § 37 havde truffet beslutning om at blokere samtlige oplysninger, der vedrørte en sag mod det pågældende barns stedfar. Højesteret udtalte, at de bilag, A havde fremsendt til landsretten, ikke kunne udelades ved fremsendelsen af hendes redegørelse til landsretten. På denne baggrund var det nødvendigt for at oplyse sagen på korrekt måde, at A tillige medtog politimesterens afgørelse om indstillingen af efterforskningen og den skrivelse fra K, hvoraf oplysningen om blokeringen fremgik. Højesteret konkluderede, at det ikke efter indhol-

[421] Persondataloven med kommentarer (2015), s. 536.
[422] Persondataloven med kommentarer (2015), s. 156 f.

det af skrivelsen fra K kunne anses for stridende mod god advokatskik, at A ikke særligt gjorde opmærksom på, at de 2 bilag indeholdt blokerede oplysninger.

4.8.3. Databeskyttelsesforordningen

Det fremgår af begrundelsen til forslaget til databeskyttelsesforordningen, at forordningens artikel 18 (som var en del af artikel 17 i forslaget) i visse tilfælde integrerer retten til at få behandlingen "begrænset", så den tvetydige terminologi "blokering" undgås[423], da denne leder tankerne hen på, at der er tale om en endelig foranstaltning, hvilket ikke er tilfældet.

Retten i forordningens artikel 18 til begrænsning er således en pendant til direktivets ret til blokering i artikel 12, litra b.

Ifølge artikel 4, nr. 3, defineres "begrænsning af behandling" som en mærkning af opbevarede personoplysninger med den hensigt at begrænse fremtidig behandling af disse oplysninger.

Det fremgår af artikel 18, at den registrerede har ret til fra den dataansvarlige at opnå begrænsning af behandling, hvis et af følgende forhold gør sig gældende:

a) Rigtigheden af personoplysningerne bestrides af den registrerede, i perioden indtil den dataansvarlige har haft mulighed for at fastslå, om personoplysningerne er korrekte.
b) Behandlingen er ulovlig, og den registrerede modsætter sig sletning af personoplysningerne og i stedet anmoder om, at anvendelsen heraf begrænses.
c) Den dataansvarlige ikke længere har brug for personoplysningerne til behandlingen, men de er nødvendige for, at et retskrav kan fastlægges, gøres gældende eller forsvares.
d) Den registrerede har gjort indsigelse mod behandlingen i medfør af artikel 21, stk. 1, i perioden mens det kontrolleres, om den dataansvarliges legitime interesser går forud for den registreredes legitime interesser.

Litra a må antages at supplere artikel 5, stk. 1, litra d, som foreskriver, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, *straks* slettes eller berigtiges. Det må således antages, at den dataansvarlige skal begrænse behandlingen, hvis den registrerede anmoder om sletning eller berigtigelse.

[423] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), s. 9.

For så vidt angår litra b må bestemmelsen ud fra en ordlydsfortolkning antages at give den registrerede en ny rettighed – ret til at *modsætte sig sletning*. Det fremgår direkte af ordlyden, at den angår ulovlig behandling, og det må antages, at den dataansvarlige som udgangspunkt ville være forpligtet til at slette oplysningerne. Denne bestemmelse kan tænkes at skulle ses i sammenhæng med forordningens artikel 82 om ret til erstatning og erstatningsansvar og vil kunne finde anvendelse, hvor den registrerede ønsker at bruge oplysningerne som bevis.

Litra c må antages at indebære en "begrænset" begrænsning af behandlingen til at angå den behandling af oplysningerne, som er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Det må i øvrigt antages, at bestemmelsen angår oplysninger, som den dataansvarlige lovligt ville kunne behandle ind til udløbet af en generel slettefrist.

Litra d supplerer retten til indsigelse og fastslår, at den dataansvarlige skal begrænse behandling af oplysninger i en periode, mens det kontrolleres, om den dataansvarliges legitime interesser går forud for den registreredes legitime interesser. Der henvises til afsnit 4.11. om forordningens artikel 21.

Om *virkningen af*, at behandlingen er blevet begrænset i medfør af artikel 18, stk. 1, fremgår det af stk. 2, at sådanne oplysninger, bortset fra opbevaring, kun må behandles med den registreredes samtykke eller med henblik på, at et retskrav kan fastlægges, gøres gældende eller forsvares, eller for at beskytte en anden fysisk eller juridisk person af hensyn til Unionens eller en medlemsstats vigtige samfundsinteresser. Begrænsning af behandling må således antages i det væsentlige at svare til blokering af oplysninger, jf. herved det ovenfor anførte om bemærkningerne til persondatalovens § 37.

Det fremgår af præambelbetragtning nr. 67, at *metoder til at begrænse behandling* af personoplysninger bl.a. kan omfatte, at udvalgte oplysninger midlertidigt flyttes til et andet behandlingssystem, at udvalgte personoplysninger gøres utilgængelige for brugere, eller at offentliggjort oplysninger midlertidigt fjernes fra et websted. I automatiske registre bør begrænsning af behandling i princippet sikres ved hjælp af tekniske midler på en sådan måde, at personoplysningerne ikke kan viderebehandles og ikke kan ændres. Det forhold, at behandling af personoplysninger er begrænset, bør angives tydeligt i systemet.

Det følger af artikel 18, stk. 3, at den dataansvarlige skal *underrette* den registrerede, inden begrænsningen af behandlingen *ophæves*.

4.8.4. Overvejelser

Bestemmelsen i artikel 18 om retten til begrænsning viderefører i vidt omfang gældende ret i databeskyttelsesdirektivets artikel 12, litra b, om "blokering". For så vidt angår samspillet med adgangen til aktindsigt efter offentlighedslovens og forvaltningsloven, henvises til afsnit 10.2. om rammerne i artikel 86 vedrørende aktindsigt i officielle dokumenter.

4.9. Underretningspligt, artikel 19

4.9.1. Præsentation

Det fremgår af persondatalovens § 37, stk. 2, at den dataansvarlige skal underrette den tredjemand, hvortil oplysningerne er videregivet, om, at de videregivne oplysninger er berigtiget, slettet eller blokeret i henhold til stk. 1, hvis en registreret person fremsætter anmodning herom. Dette gælder dog ikke, hvis underretningen viser sig umulig eller er uforholdsmæssigt vanskelig.

Databeskyttelsesforordningens artikel 19 indeholder en nogenlunde tilsvarende bestemmelse, som dog indeholder nogle yderligere krav til den dataansvarlige i forbindelse med underretningspligten.

Det følger af bestemmelsen, at den dataansvarlige underretter hver modtager, som personoplysningerne er videregivet til, om enhver berigtigelse eller sletning af personoplysningerne eller begrænsning af behandling, der er udført i henhold til artikel 16, artikel 17, stk. 1, og artikel 18, medmindre dette viser sig umuligt eller er uforholdsmæssigt vanskeligt. Den dataansvarlige oplyser den registrerede om disse modtagere, hvis den registrerede anmoder herom.

4.9.2. Gældende ret

Det fremgår af persondatalovens § 37, stk. 2, at den dataansvarlige skal underrette den tredjemand, hvortil oplysningerne er videregivet, om, at de videregivne oplysninger er berigtiget, slettet eller blokeret i henhold til stk. 1, hvis en registreret person fremsætter anmodning herom. Dette gælder dog ikke, hvis underretningen viser sig umulig eller er uforholdsmæssigt vanskelig.

Bestemmelsen er baseret på databeskyttelsesdirektivets artikel 12, litra c, hvoraf det fremgår, at medlemsstaterne sikrer enhver registreret ret til hos den dataansvarlige at få udvirket, at tredjemand, til hvem sådanne oplysninger er blevet videregivet, underrettes om enhver berigtigelse, sletning eller blokering, der er foretaget i overensstemmelse med litra b, medmindre underretning viser sig umulig eller er uforholdsmæssig vanskelig.

Det er vigtigt at være opmærksom på, at persondatalovens § 37, stk. 2, kun finder anvendelse i de situationer, hvor det er blevet fastslået, at f.eks. en myndighed behandler urigtige eller vildledende oplysninger om den registrerede. Bestemmelsen finder således ikke anvendelse, hvis der er tale om korrekte oplysninger. En sådan behandling vil i stedet kunne forhindres efter persondatalovens 5, stk. 1, om god databehandlingsskik.

Det fremgår af bemærkningerne til persondataloven, at en anmodning om underretning af tredjemand skal komme fra den registrerede eller dennes fuldmægtig. Anmodningen, der kan fremsættes formløst, skal angå oplysninger om den registrerede selv. Den dataansvarlige er således ikke forpligtet til efter anmodning at foretage underretning af tredjemand, hvis der er tale om behandling af oplysninger om andre personer.[424] Datatilsynet har dog anført, at for så vidt angår offentlige myndigheder, vil en sådan pligt kunne følge af begrebet god forvaltningsskik.[425]

Det fremgår endvidere af bemærkningerne til persondataloven, at hvis anmodning fremsættes, påhviler det den dataansvarlige eller dennes repræsentant snarest muligt at tage stilling til, om begæringen kan imødekommes og i givet fald at underrette de tredjemænd, hvortil oplysninger om den registrerede er videregivet. Der gælder ikke formkrav til den dataansvarliges underretning. Derimod stilles der krav om, at det i underretningen angives, hvilken korrigeringsmetode den dataansvarlige har anvendt for at imødekomme en berettiget anmodning fra den registrerede, jf. persondatalovens § 37, stk. 1. Heri ligger endvidere, at der skal gives tredjemand underretning om anledningen til, at berigtigelse, sletning eller blokering har fundet sted.[426]

Endelig fremgår det af bemærkningerne til persondataloven, at i de tilfælde, hvor der er sket en berigtigelse af eksempelvis urigtige eller vildledende oplysninger, vil det oftest være nødvendigt, at underretningen omfatter såvel de tidligere afgivne, fejlagtige oplysninger som de nye, rigtige oplysninger. Hvis eksempelvis der er tale om, at de videregivne oplysninger er fejlagtige med hensyn til den oplysning, som modtageren anvender som søgenøgle, f.eks. navn eller personnummer, er det således nødvendigt, at også den oprindelige – fejlagtige – oplysning angives, hvorved modtageren af underretningen i praksis kan foretage berigtigelse mv. af oplysningerne.[427]

---

[424] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[425] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.3.1.
[426] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.
[427] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 37.

Det følger af persondatalovens § 37, stk. 2, 2. pkt., at pligten til underretning af de tredjemænd, hvortil korrigerede oplysninger er videregivet, ikke gælder, hvis underretningen viser sig umulig eller er uforholdsmæssigt vanskelig.

Det fremgår herom af Datatilsynets vejledning om registreredes rettigheder, at i hvilket omfang, dette vil være tilfældet, vil bero på en afvejning af på den ene side betydningen af underretningen for den registrerede, og på den anden side den arbejdsindsats hos den dataansvarlige, som vil være forbundet med en sådan underretning. Der skal foretages en afvejning i hvert enkelt tilfælde af alle de momenter, som kan tillægges vægt i vurderingen af de nævnte modsatrettede hensyn. Under hensyntagen til at den registrerede selv skal anmode om, at der gives underretning til de tredjemænd, som har modtaget urigtige eller vildledende oplysninger om vedkommende, vil det i almindelighed skulle lægges til grund, at det er af stor betydning for den registrerede, at sådan underretning gives. Da det endvidere oftest ikke vil være forbundet med store arbejdsmæssige eller ressourcemæssige belastninger for den dataansvarlige at foretage underretning, vil underretning derfor som hovedregel skulle gives. Der skal med andre ord anføres tungtvejende argumenter for, at den dataansvarlige kan undlade at give underretning.[428]

4.9.3. Databeskyttelsesforordningen

Det fremgår af databeskyttelsesforordningens artikel 19, at den dataansvarlige underretter hver modtager, som personoplysningerne er videregivet til, om enhver berigtigelse eller sletning af personoplysningerne eller begrænsning af behandling, der er udført i henhold til artikel 16, artikel 17, stk. 1, og artikel 18, medmindre dette viser sig umuligt eller er uforholdsmæssigt vanskeligt. Den dataansvarlige oplyser den registrerede om disse modtagere, hvis den registrerede anmoder herom.

For så vidt angår ordlyden i forordningens artikel 19, i forhold til persondatalovens § 37, stk. 2, og databeskyttelsesdirektivets artikel 12, litra c, ses indholdet på baggrund af en ordlydsfortolkning at være nogenlunde identisk – dog er der i databeskyttelsesforordningen nogle yderligere krav til den dataansvarlige.

I databeskyttelsesdirektivet knytter underretningspligten sig til artikel 12, litra b, og de forskellige muligheder for berigtigelse, sletning eller blokering, som følger heraf. Ligesom underretningspligten i persondatalovens § 37, stk. 2, knytter sig til persondatalovens § 37, stk. 1. Databeskyttelsesforordningens underretningspligt knytter sig til de næsten tilsvarende bestemmelser i forordningens artikel 16, 17, stk. 1 og 18, som dog ikke er helt identiske med bestemmelserne i databeskyttelsesdirektivet og persondataloven. Selvom underret-

[428] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.3.2.

ningspligten knytter sig til ikke helt identiske metoder til at korrigere urigtige personoplysninger, så ses kravet om at underrette modtagerne efter databeskyttelsesforordningen at være nogenlunde identisk med gældende ret.

Der er i persondatalovens § 37, stk. 2 og i databeskyttelsesdirektivets artikel 12, litra c, dog en tilføjelse om, *hvis en registreret person fremsætter anmodning herom*, som ikke fremgår af databeskyttelsesforordningen. Som anført ovenfor, vil den underretning, som den dataansvarlige giver efter gældende ret, således kun skulle ske, hvis den registrerede fremsætter anmodning herom.

Databeskyttelsesforordningens artikel 19 indeholder en ændring heraf. Efter forordningens ordlyd vil den underretning, som sker efter forordningens artikel 19, skulle ske på den dataansvarliges eget initiativ. Efter bestemmelsen vil det derfor ikke være et krav, at den registrerede anmoder om underretningen. Det påhviler således den dataansvarlige at foranledige, at der sker den fornødne underretning af de modtagere, som personoplysningerne er videregivet til.

Datatilsynet antager som tidligere anført, at i vurderingen af om en underretning er umulig eller uforholdsmæssig vanskelig, skal der tungtvejende argumenter for, at den dataansvarlige kan undlade at give underretning. Datatilsynet tillægger det her betydning, at den registrerede selv skal anmode om, at der gives underretning til de tredjemænd, som har modtaget urigtige eller vildledende oplysninger om vedkommende, hvorfor det i almindelighed vil skulle lægges til grund, at det er af stor betydning for den registrerede, at sådan underretning gives.

Datatilsynet anfører dog som tidligere anført tillige, at da det oftest ikke vil være forbundet med store arbejdsmæssige eller ressourcemæssige belastninger for den dataansvarlige at foretage underretning, vil underretning derfor som hovedregel skulle gives. Det samme vil være tilfældet i forbindelse med den underretning, som skal gives efter databeskyttelsesforordningen. I forhold til afvejningen af, hvornår en underretning viser sig umulig eller uforholdsmæssigt vanskelig, må forordningen således ses at være en videreførelse af gældende ret og praksis fra Datatilsynet.

I databeskyttelsesforordningen er der endnu en tilføjelse til bestemmelsen i artikel 19, hvoraf det følger, at den dataansvarlige oplyser den registrerede om disse modtagere, hvis den registrerede anmoder herom. Dette krav om oplysning af den registrerede følger ikke direkte af hverken databeskyttelsesdirektivet eller persondataloven, hvorfor der vil være tale om et nyt yderligere krav, som påhviler den dataansvarlige i forbindelse med underretning om berigtigelse, sletning eller begrænsning af behandling. Dette harmonerer dog med,

at underretningen efter forordningen skal ske på den dataansvarliges og ikke den registreredes initiativ.

Overordnet ses databeskyttelsesforordningens artikel 19, således at være i overensstemmelse med gældende ret – dog vil det efter forordningen nu være den dataansvarlige, som på eget initiativ skal foretage underretning af modtagerne, ligesom der i tilknytning hertil vil skulle ske oplysning om modtagerne til den registrerede, hvis den registrerede anmoder herom.

4.9.4. Overvejelser

Databeskyttelsesforordningens artikel 19 er overordnet en videreførelse af gældende ret – dog vil det efter forordningen nu være den dataansvarlige, som på eget initiativ skal foretage underretning af modtagerne, ligesom der i tilknytning hertil vil skulle ske oplysning om modtagerne til den registrerede, hvis den registrerede anmoder herom.

4.10. Retten til dataportabilitet, artikel 20

4.10.1. Præsentation

Ved forordningens artikel 20 indføres en ny rettighed for den registrerede til dataportabilitet, som indebærer en ret til i visse tilfælde at modtage personoplysninger – som vedkommende har givet til en dataansvarlig – om sig selv i et struktureret, almindeligt anvendt og maskinlæsbart format. Herudover indebærer retten til dataportabilitet en rettighed for den registrerede til i visse tilfælde at få transmitteret disse oplysninger om sig selv fra én dataansvarlig til anden uden hindring fra den dataansvarlige, som personoplysningerne er blevet givet til.

Formålet med denne nye rettighed er at øge den registreredes kontrol over egne personoplysninger ved at fremme mulighederne for let at få flyttet, kopieret eller overført vedkommendes personoplysninger til sig selv eller fra én tjenesteudbyder til en anden.

Retten til dataportabilitet finder ikke anvendelse på behandling, der er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, jf. artikel 20, stk. 3, 2. pkt.

4.10.2. Gældende ret

En lignende bestemmelse findes ikke i databeskyttelsesdirektivet eller persondataloven. Men tankegangen om portabilitet er ikke ny og kan ses på en række andre områder. Det

drejer sig f.eks. om kommunikationsservices og ved regulering af visse kontrakters udløb.[429]

4.10.3. Databeskyttelsesforordningen

Som nævnt indføres der med forordningens artikel 20 en ny rettighed for de registrerede til dataportabilitet.

Det fremgår af forordningens artikel 20, stk. 1, at den registrerede i visse tilfælde har ret til i et struktureret, almindeligt anvendt og maskinlæsbart format at modtage personoplysninger om sig selv, som vedkommende har givet til en dataansvarlig, og har ret til at få transmittere disse oplysninger til en anden dataansvarlig uden hindring fra den dataansvarlige, som personoplysningerne er blevet givet til.

Det fremgår af forordningens præambelbetragtning nr. 68, at formålet med retten til dataportabilitet er at øge den registreredes kontrol over sine personoplysninger. Herudover fremgår det af samme præambelbetragtning, at dataansvarlige bør opfordres til at udvikle indbyrdes kompatible formater, der muliggør dataportabilitet.

Artikel 29-gruppen har udtalt, at formålet med retten til dataportabilitet er at give de registrerede kontrol over deres egne oplysninger, da retten letter deres adgang til at flytte og kopiere eller transmittere personoplysninger fra et IT-miljø til et andet.[430]

Retten til dataportabilitet består som nævnt af retten for den registrerede til henholdsvis at modtage egne oplysninger i et struktureret, almindeligt anvendt og maskinlæsbart format og retten til at få transmitteret disse oplysninger fra én dataansvarlig til en anden uden hindring.

Som eksempel på den registreredes mulighed for at modtage egne oplysninger til eget brug anfører Artikel 29-gruppen[431], at retten til dataportabilitet f.eks. muliggør, at den registrerede kan modtage en liste over sine kontaktpersoner fra den pågældendes webmail-udbyder eller modtage en eksisterende spilleliste med musik fra den pågældendes musikstreamingstjeneste i et struktureret, almindeligt anvendt og maskinlæsbart format.

Retten til dataportabilitet giver således mulighed for, at den registrerede på en ubesværet måde kan *modtage* og dermed bruge og videreanvende oplysninger om sig selv til egne

[429] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 4.

[430] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 4.
[431] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 5.

formål, som denne ellers havde givet til en dataansvarlig. Herudover indebærer retten til dataportabilitet en ret for den registrerede til at få *transmitteret* personoplysninger om sig selv fra én dataansvarlig til en anden uden hindring fra den dataansvarlige. Det betyder, at den registrerede ikke blot har ret til at modtage og genanvende sine personoplysninger til egne formål, men også til at få *transmitteret* de angivne oplysninger fra én tjenesteudbyder til en anden uden hindringer.[432]

For så vidt angår ansvaret for databehandlingen, udtaler Artikel 29-gruppen, at den dataansvarlige, som overfører oplysninger på baggrund af en anmodning om dataportabilitet, ikke skal anses for ansvarlig for den behandling af den registreredes personoplysninger, som den registrerede selv eller den modtagende dataansvarlige foretager.[433]

I stedet er det den modtagende dataansvarlige, som er ansvarlig for behandlingen af den registreredes personoplysninger og dermed er forpligtet til at efterleve forordningens regler, herunder artikel 5 om principper for behandling af personoplysninger. Som eksempel herpå nævner Artikel 29-gruppen[434] situationen, hvor den registrerede anmoder om overførsel af egne oplysninger fra én webmail-udbyder til en anden, såsom til en sikker opbevaringsplatform. I et sådant tilfælde kan den registreredes oplysninger fra webmailen indeholde kontaktoplysninger på den registreredes kontakter, dvs. oplysninger om andre personer end den registrerede. Ifølge Artikel 29-gruppen bør den modtagende dataansvarlige hverken behandle eller beholde disse oplysninger fra andre registrerede, hvis oplysningerne ikke er relevante i forhold til formålet med behandlingen af personoplysningerne om den registrerede. Det samme gør sig gældende for portabilitet af oplysninger om den registreredes bankoverførsler.[435]

Herudover udtaler Artikel 29-gruppen, at retten til dataportabilitet ikke medfører en forpligtelse for den tidligere dataansvarlige til at beholde den registreredes personoplysninger længere end nødvendigt blot for at imødekomme en fremtidig anmodning om dataportabilitet.[436]

Det fremgår af forordningens artikel 20, stk. 3, 1. pkt., at udøvelsen af retten til dataportabilitet, ikke berører retten til sletning (retten til at blive glemt) efter forordningens artikel 17. Det betyder, at den dataansvarlige ikke kan påberåbe sig den registreredes ret til data-

[432] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 5.
[433] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 6.
[434] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 6.
[435] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 6-7.
[436] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 6.

portabilitet som begrundelse for enten at afvise eller forsinke den registreredes ret til sletning eller til at blive glemt i medfør af forordningens artikel 17.[437]

Endelig fremgår det af forordningens artikel 20, stk. 2, at når den registrerede udøver sin ret til dataportabilitet, har den registrerede ret til at få transmitteret personoplysninger direkte fra en dataansvarlig til en anden, hvis det er teknisk muligt.

4.10.3.1. Betingelser for retten til dataportabilitet
Det fremgår af forordningens artikel 20, stk. 1 og 4, at tre kumulative betingelser skal være opfyldt, førend den registrerede har ret til dataportabilitet.

For det første skal behandlingen af personoplysninger være omfattet af betingelserne i artikel 20, stk. 1, *litra a* og *litra b*.

Dernæst skal de personoplysninger, som ønskes overført, omhandle den registrerede selv, og vedkommende skal have givet disse oplysninger til en dataansvarlig, jf. artikel 20, stk. 1.

Endelig må retten til dataportabilitet ikke krænke andres rettigheder eller frihedsrettigheder, jf. artikel 20, stk. 4.

4.10.3.2. Krav til selve behandlingen af personoplysninger, artikel 20, stk. 1, litra a og litra b
For det første fremgår det af forordningens artikel 20, stk. 1, *litra a*, at den registrerede har ret til dataportabilitet, når behandlingen af den registreredes personoplysninger enten er baseret på den registreredes *samtykke* eller er nødvendig for opfyldelsen af en *kontrakt*.

For så vidt angår behandling af personoplysninger på baggrund af den registreredes *samtykke* betyder det, at behandling, der foretages i medfør af forordningens artikel 6, stk. 1, litra a, eller artikel 9, stk. 2, litra a, er omfattet af den registreredes ret til dataportabilitet, jf. artikel 20, stk. 1, *litra a*.

For så vidt angår behandling af personoplysninger på baggrund af en *kontrakt*, som den registrerede er part i, betyder det, at behandling, der foretages i medfør af forordningens artikel 6, stk. 1, litra b, er omfattet af den registreredes ret til dataportabilitet, jf. artikel 20, stk. 1, *litra a*.

[437] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 7.

Som praktiske eksempler på situationer hvor en behandling af den registreredes personoplysninger sker på baggrund af en kontrakt, som den registrerede er part i, nævner Artikel 29-gruppen bl.a. oversigter over de bogtitler, den registrerede har købt fra en online boghandler eller en liste over de sange, den registrerede har lyttet til via en musikstreamingstjeneste.[438]

Artikel 29-gruppen har endvidere udtalt, at en finansiel virksomhed f.eks. ikke har pligt til at imødekomme en anmodning om dataportabilitet, hvis virksomheden behandler oplysninger om den registrerede som følge af dennes forpligtelser efter f.eks. regler om hvidvask.[439]

Dermed gælder retten til dataportabilitet ikke, hvis behandlingen af personoplysninger er baseret på *et andet retsgrundlag* end samtykke eller kontrakt. Det fremgår endvidere af præambelbetragtning nr. 68, at retten til dataportabilitet på grund af sin karakter ikke bør udøves over for dataansvarlige, der behandler personoplysninger under udøvelsen af deres offentlige opgaver eller hvis behandling af personoplysninger er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.

Herudover fremgår det af forordningens artikel 20, stk. 3, *2. pkt.*, at retten til dataportabilitet ikke finder anvendelse på behandling, der er nødvendig for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Opgaver i samfundets interesse kan for eksempelvis være opgaver af almen interesse, dvs. opgaver, som er af betydning for en bredere kreds af personer. Dette vil bl.a. være tilfældet for så vidt angår behandling i statistisk, historisk eller videnskabeligt øjemed. Endvidere kan nævnes den behandling, som sker i retsinformationssystemer med henblik på at informere offentligheden om lovgivning, retspraksis mv. Også andre former for behandling vil kunne anses for at være af almen interesse. Dette gælder f.eks. større private foreningers og sammenslutningers registreringer af oplysninger, som er af interesse for en bredere kreds af personer. Det forhold, at behandling sker i et kommercielt øjemed udelukker ikke, at behandlingen anses for at ske til varetagelse af almene interesser.[440]

Selvom den registrerede i disse tilfælde ikke vil kunne påberåbe sig retten til dataportabilitet, vil de øvrige rettigheder efter forordningen finde anvendelse, herunder retten til indsigt.

[438] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 8.
[439] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 8.
[440] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 6.

Dernæst fremgår det af forordningens artikel 20, stk. 1, *litra b*, at behandlingen skal foretages automatisk, førend den registrerede har ret til dataportabilitet. Det betyder f.eks., at oplysninger, der behandles manuelt ikke er omfattet af den registreredes ret til dataportabilitet.

4.10.3.3. Krav til de pågældende personoplysninger, artikel 20, stk. 1
Det følger af artikel 20, stk. 1, at retten til dataportabilitet omfatter *personoplysninger om den registrerede selv*, *som vedkommende har givet til en dataansvarlig.*

Der skal således være tale om *personoplysninger*, hvilket vil sige enhver form for information om en identificerbar fysisk person, jf. definitionen i forordningens artikel 4, nr. 1. Omvendt betyder det, at anonymiserede oplysninger ikke er omfattet af bestemmelsen.

Herudover skal der være tale om *personoplysninger om den registrerede selv*. Personoplysninger om den registrerede kan til tider også indeholde personoplysninger om andre registrerede personer, såsom fortegnelser over telefonoplysninger, som kan indeholde opkaldslister, der omfatter oplysninger om indgående og udgående opkald fra andre registrerede personer.

I forhold til denne problemstilling udtaler Artikel 29-gruppen, at der ikke skal anvendes en for snæver fortolkning af betegnelsen "*personoplysninger om den registrerede selv"*.[441] Artikel 29-gruppen nævner herefter eksemplet med fortegnelser over telefonoplysninger, der ifølge Artikel 29-gruppen skal anses for omfattet af personoplysninger *om den registrerede selv*, selvom disse kan indeholde oplysninger om andre registrerede personer. Hertil skal det bemærkes, at den behandling af personoplysninger, som den modtagende dataansvarlige foretager, ikke må krænke andres rettigheder eller frihedsrettigheder, jf. forordningens artikel 20, stk. 4.

Dernæst er det et krav, at *vedkommende selv har givet disse oplysninger til en dataansvarlig*. Dette kan f.eks. omfatte oplysninger, som den registrerede har givet til den dataansvarlige via en formular på internettet, såsom f.eks. kontaktoplysninger og brugernavn ved oprettelse af en profil eller internetkøb mv.

Som undtagelse hertil nævner Artikel 29-gruppen, at de oplysninger, som den dataansvarlige har *skabt* på baggrund af de oplysninger, som den registrerede har givet til den dataan-

[441] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 8-9.

svarlige, *ikke* skal anses for omfattet af retten til dataportabilitet.[442] Sådanne "udledte oplysninger" kan f.eks. bestå af den dataansvarliges analyser eller anden bearbejdning på baggrund af den registreredes adfærd eller aktivitet, såsom oplysninger om kreditvurdering, personaliserede anbefalinger på webshops genereret ud fra forbrugerens tidligere køb eller helbredsvurdering på baggrund af brugen af en fitness-applikation eller andre resultater fra en algoritme mv.

4.10.3.4. Artikel 20, stk. 4

Endelig fremgår det af artikel 20, stk. 4, at det er en betingelse for retten til dataportabilitet, at denne ikke må krænke andres rettigheder eller frihedsrettigheder.

Såfremt en overførsel af personoplysninger fra én tjenesteudbyder til en anden i overensstemmelse med den registreredes ret til dataportabilitet forhindrer, at en tredjepart kan udøve sin ret til f.eks. indsigt eller information efter forordningen, finder retten til dataportabilitet således ikke anvendelse.[443]

Herudover skal det bemærkes, at den modtagende dataansvarlige skal have hjemmelsgrundlag i forordningen til både at behandle oplysningerne om den registrerede og eventuelle oplysninger om andre personer. For så vidt angår hjemmelsgrundlaget for behandling af den registreredes oplysninger, vil dette normalt ske på baggrund af enten samtykke eller kontrakt i medfør af forordningens artikel 6, stk. 1, litra a, eller artikel 9, stk. 2, litra a, eller artikel 6, stk. 1, litra b.

Behandlingen af oplysninger om andre personer end den registrerede må antages særligt at kunne foretages, hvis det er nødvendigt for, at den dataansvarlige eller tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn, jf. artikel 6, stk. 1, litra f.

Som eksempel herpå nævner Artikel 29-gruppen[444] spørgsmålet om overførsel af oplysninger fra én bank til en anden. De overførte oplysninger fra en bank kan bl.a. bestå af oplysninger om transaktioner til og fra andre personer end den registrerede. I et sådant tilfælde må det ifølge Artikel 29-gruppen antages at være usandsynligt, at de andre registreredes

[442] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 10-11.
[443] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 12.
[444] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 12.

rettigheder og frihedsrettigheder påvirkes negativt, såfremt oplysningerne anvendes til det samme formål.[445]

For at undgå negative konsekvenser for de tredjeparter, hvis oplysninger kan være omfattet af retten til dataportabilitet, udtaler Artikel 29-gruppen, at den modtagende dataansvarlige alene må behandle de pågældende oplysninger til det samme formål. Dermed må den dataansvarlige ikke anvende disse oplysninger til egne formål, såsom til at tilbyde marketingprodukter og services rettet til de pågældende tredjeparter.[446]

Det skal endvidere bemærkes, at forbuddet efter artikel 20, stk. 4, også omfatter forretningshemmeligheder eller intellektuel ejendomsret, navnlig ophavsret.[447]

Til dette bemærker Artikel 29-gruppen dog, at potentielle forretningsrisici ikke i sig selv kan danne grundlag for at afvise retten til dataportabilitet.[448] Dette gælder ligeledes afvisning af retten til dataportabilitet som følge af mulig overtrædelse af andre kontraktuelle rettigheder, såsom en udestående gæld mv. I stedet anbefales det, at den dataansvarlige overfører de personoplysninger, som den registrerede selv har givet på en sådan måde, så forretningshemmeligheder mv. ikke omfattes af disse.

For så vidt angår forholdet til medlemsstaternes nationale lovgivning, som giver mulighed for en form for overførsel af personoplysninger, udtaler Artikel 29-gruppen, at der i disse tilfælde også skal tages hensyn til betingelserne i den nationale lovgivning, når retten til dataportabilitet efterleves.[449] Artikel 29-gruppen anfører endvidere, at i tilfælde, hvor det er klart ud fra den registreredes anmodning, at der ikke er tale om en udøvelse af retten til dataportabilitet, men en ret, der følger af en medlemsstats national lovgivning, finder forordningens regler om dataportabilitet som udgangspunkt ikke anvendelse på anmodningen.

4.10.3.5. Formateringskrav

Det fremgår af artikel 20, stk. 1, at de overførte oplysninger skal være i et struktureret, almindeligt anvendt og maskinlæsbart format.

[445] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 12.
[446] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 13.
[447] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 13.
[448] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 13.
[449] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 7-8.

Det fremgår endvidere af præambelbetragtning nr. 68, at de overførte oplysninger skal være i et indbyrdes kompatibelt format. Derudover fremgår det af databeskyttelsesforordningens præambelbetragtning nr. 68, at den registreredes ret til at transmittere eller modtage personoplysninger vedrørende vedkommende ikke bør skabe en forpligtelse for dataansvarlige til at indføre eller opretholde behandlingssystemer, som er teknisk kompatible. Det må antages at betyde, at retten til dataportabilitet fordrer interoperabilitetsløsninger, men at dette ikke medfører et selvstændigt krav om at sikre teknisk kompatible systemer.[450]

For så vidt angår begrebet "indbyrdes kompatibelt format", anvendes begrebet "interoperable format" i den engelske sprogversion af forordningen, som kan oversættes til "interoperabilitet", der er et EU-retligt begreb. Det fremgår således af artikel 2 i Europa-Parlamentets og Rådets afgørelse nr. 922/2009/EF om interoperabilitetsløsninger for offentlige myndigheder, at interoperabilitet defineres som det forhold, at adskilte og forskelligartede organisationer er i stand til at interagere med henblik på at nå gensidigt fordelagtige og vedtagne fælles mål, herunder også, at organisationerne udveksler information og viden via de forretningsprocesser, de understøtter, og gennem dataudveksling mellem deres respektive IKT-systemer.

Herudover er det et krav, at oplysningerne skal være i et "struktureret", "almindeligt anvendt" og maskinlæsbart" format.

For så vidt angår "maskinlæsbart" format, er dette et EU-retligt begreb. Det fremgår således af præambelbetragtning nr. 21 i direktiv 2013/37/EU om videreanvendelse af den offentlige sektors informationer, at et dokument bør betragtes som værende i et maskinlæsbart format, hvis der er tale om data kodet i filer, der er struktureret i et maskinlæsbart format.

Artikel 29-gruppen bemærker, at der ikke i forordningen angives specifikke anbefalinger til selve formatet, men at det må antages, at valget i forhold til formatet skal foretages med "operationalitet" for øje samt at give den registrerede en stor grad af dataportabilitet.[451] Endvidere bemærker Artikel 29-gruppen, at formater, der er genstand for omkostningsfulde licenser, ikke kan anses for en hensigtsmæssig fremgangsmåde i forhold til formatet.

[450] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 18.
[451] Artikel 29-gruppens udtalelse nr. 242/2016 Guidelines on the right to data portability (WP 242 rev 1), s. 18.

4.10.4. Overvejelser

Databeskyttelsesforordningen artikel 20 om dataportabilitet er ny i forhold til databeskyttelsesdirektivet, idet den skaber en ny rettighed for den registrerede til at få overført egne oplysninger til sig selv eller fra én dataansvarlig til en anden, uden hindringer fra den dataansvarlige.

4.11. Ret til indsigelse, artikel 21

4.11.1. Præsentation

Efter persondatalovens § 35 kan den registrerede over for den dataansvarlige gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling. Hvis en sådan indsigelse er berettiget, må behandlingen ikke længere omfatte de pågældende oplysninger. Endvidere er der i persondatalovens § 36 fastsat særlige regler for de registreredes ret til indsigelse ved markedsføring.

Databeskyttelsesforordningen indeholder en tilsvarende bestemmelse i artikel 21, hvorefter den registrerede har ret til at gøre indsigelse mod bl.a. behandling af sine personoplysninger baseret på artikel 6, stk. 1, litra e eller f, og behandling med henblik på direkte markedsføring. Den dataansvarlige må herefter påvise vægtige grunde til behandlingen, der går forud for den registreredes interesser, rettigheder og frihedsrettigheder, eller påvise, at behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares, førend behandlingen kan fortsætte.

Efter databeskyttelsesforordningens artikel 21 vil den registrerede dog have en mere begrænset ret til at gøre indsigelse end efter persondatalovens §§ 35 og 36.

4.11.2. Gældende ret

4.11.2.1. Persondatalovens § 35

Det fremgår af persondatalovens § 35, stk. 1, at den registrerede til enhver tid over for den dataansvarlige kan gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling.

Persondatalovens § 35, stk. 1, fastslår således, at den registrerede kan gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling, men vurderingen af, hvornår den dataansvarlige skal efterkomme indsigelsen, må afgøres på baggrund af bestemmelsen i stk. 2.

Det fremgår af persondatalovens § 35, stk. 2, at hvis indsigelsen efter stk. 1 er berettiget, må behandlingen ikke længere omfatte de pågældende oplysninger.

Bestemmelsen er baseret på databeskyttelsesdirektivets artikel 14, litra a, hvoraf det fremgår, at medlemsstaterne indrømmer den registrerede ret til i det mindste i de i artikel 7, litra e og f, omhandlede tilfælde af vægtige legitime grunde, der vedrører den pågældendes særlige situation, til enhver tid at gøre indsigelse mod, at personoplysninger om den pågældende selv gøres til genstand for behandling, medmindre andet er bestemt i den nationale lovgivning. I tilfælde af berettiget indsigelse må den af den dataansvarlige iværksatte behandling ikke længere omfatte de pågældende oplysninger.

Det fremgår endvidere af databeskyttelsesdirektivets artikel 14, litra b, at medlemsstaterne indrømmer den registrerede ret til efter anmodning og uden udgifter at modsætte sig en behandling af personoplysninger, der vedrører den pågældende, og som den dataansvarlige agter at foretage med henblik på markedsføring, eller at blive underrettet, inden personoplysningerne første gang videregives til tredjemand eller anvendes på tredjemands vegne med henblik på markedsføring, og udtrykkeligt få tilbud om uden udgifter at gøre indsigelse mod en sådan videregivelse eller anvendelse. Der henvises i den forbindelse til afsnit 4.11. om ret til indsigelse i forbindelse med direkte markedsføring, artikel 21, stk. 2-3.

Det fremgår af præambelbetragtning nr. 45 til databeskyttelsesdirektivet, at hvor behandling af personoplysninger kan foregå fuldt lovligt i almenvellets interesse, af hensyn til offentlig myndighedsudøvelse eller i en persons legitime interesse, bør enhver ikke desto mindre være berettiget til, hvis den pågældende på grund af egne særlige forhold har tungtvejende og legitime grunde hertil at gøre indsigelse mod, at oplysningerne om den pågældende selv gøres til genstand for behandling. Medlemsstaterne har imidlertid mulighed for at vedtage nationale bestemmelser om det modsatte.

Databeskyttelsesdirektivets artikel 14, litra a, fastsætter, hvad der som minimum skal gives ret til indsigelse i. Dette harmonerer også med, at Registerudvalget i betænkning nr. 1345 udtalte, at visse af databeskyttelsesdirektivets bestemmelser også efter deres eget indhold må antages at være minimumsbestemmelser i den forstand, at Danmark kan fastsætte regler, som giver registrerede personer en bedre beskyttelse af den personlige integritet, end hvad der følger af direktivet. Dette gælder eksempelvis bestemmelsen i artikel 14, stk. 1, litra a, om den registreredes indsigelsesret, jf. bestemmelsens ordlyd om "i det mindste".[452]

[452] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 33.

Registerudvalget foreslog i betænkning nr. 1345, at § 35, stk. 1, i den danske persondatalov skulle have følgende udformning: *Den registrerede kan, hvor vægtige grunde, der vedrører den pågældendes særlige situation, taler derfor, til enhver tid over for den dataansvarlige gøre indsigelse mod, at oplysninger om den pågældende gøres til genstand for behandling i medfør af bestemmelserne i § 6, nr. 5-7.* Endvidere indeholdt bestemmelsens stk. 2 en undtagelse, hvorefter stk. 1 ikke fandt anvendelse, hvis behandlingen var foreskrevet i lovgivningen eller skete i statistisk eller videnskabeligt øjemed.

Registerudvalget anførte vedrørende den foreslåede § 35, at bestemmelsen måtte antages at skulle forstås således, at den alene omfattede de tilfælde, hvor behandling af oplysninger var lovlig efter bestemmelserne i direktivet. I disse tilfælde skulle der efter bestemmelsen gives den registrerede ret til under nærmere angivne betingelser at gøre indsigelse mod behandlingen af oplysninger. Uden for bestemmelsens område faldt dermed de situationer, hvor behandling af oplysninger skete i strid med direktivets materielle behandlingsregler. For sådanne situationer gjaldt imidlertid naturligvis også, at den registrerede kunne rette henvendelse til den dataansvarlige (og efter omstændighederne eventuelt tilsynsmyndigheden) med henblik på at påpege, at ulovlig behandling af oplysninger om den pågældende fandt sted. I det omfang dette var tilfældet, ville fortsat behandling af oplysningerne naturligvis ikke kunne ske.[453]

Registerudvalget anførte endvidere i betænkning nr. 1345, at der ikke var grundlag for at udstrække den registreredes indsigelsesret til at gælde for den behandling af oplysninger, som skete i henhold til direktivets øvrige materielle behandlingsregler. Eksempelvis burde der ikke kunne gøres indsigelse mod behandling af oplysninger, der er nødvendig for at overholde en retlig forpligtelse, som gælder for den dataansvarlige, jf. artikel 7, litra c. I modsat fald ville der nemlig bl.a. kunne gøres indsigelse mod, at oplysninger behandledes i forbindelse med domstolenes behandling af civile retssager.[454]

Registerudvalget anførte i betænkning nr. 1345 således vedrørende den tidligere foreslåede § 35, at i de tilfælde, hvor behandlingen af oplysninger skete i henhold til udkastets § 6, nr. 1-4, ville den registrerede ikke efter bestemmelsen kunne gøre indsigelse mod behandlingen.[455]

Både ved forslag nr. L 82, fremsat den 30. april 1998, til lov om behandling af personoplysninger og forslag nr. L 44, fremsat den 8. oktober 1998, til lov om behandling af per-

[453] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 318.
[454] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 319.
[455] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 488.

sonoplysninger, som gik forud for den nuværende persondatalov, havde persondatalovens § 35 den af Registerudvalget foreslåede udformning.

Ved forslag nr. L 147, fremsat den 9. december 1999, til lov om behandling af personoplysninger blev lovens § 35 ændret således, at det udtrykkeligt i lovteksten blev fastsat, at den registrerede til enhver tid kan gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling. Persondatalovens § 35 fik herved dens nuværende udformning.

I forbindelse med fremsættelse af forslag nr. L 147 anførte Justitsministeriet, at ministeriet i det væsentlige kunne tilslutte sig udvalgets forslag om, at den registrerede – når vægtige grunde, der vedrører den pågældendes særlige situation, taler derfor – skal kunne gøre indsigelse mod, at oplysninger om den pågældende gøres til genstand for behandling i medfør af lovforslagets § 6, nr. 5-7. Efter Justitsministeriets opfattelse burde den dataansvarliges pligt til efter omstændighederne at ophøre med en i øvrigt lovlig behandling, som den registrerede har gjort indsigelse imod, i princippet ikke være begrænset til behandlinger, der foretages i medfør af bestemmelserne i § 6, nr. 5-7. Justitsministeriet fandt endvidere, at informative grunde talte for, at det fremgik direkte af lovteksten, at den registrerede til enhver tid kan gøre indsigelse mod en behandling, således at den dataansvarlige er forpligtet til at tage stilling til, om indsigelsen er berettiget.[456]

I persondatalovens § 35 er det således fastsat, at den registrerede kan gøre indsigelse mod alle behandlinger, uanset efter hvilken bestemmelse oplysningerne behandles. Anvendelsesområdet efter persondataloven ses derfor at være bredere end, hvad der følger af databeskyttelsesdirektivet.

Datatilsynet anfører i vejledning om registreredes rettigheder, at en indsigelse mod en behandling af personoplysninger naturligvis vil være berettiget, hvis behandlingen ikke er lovlig, dvs. finder sted i *strid med reglerne i persondataloven eller anden lovgivning.*[457]

En indsigelse vil imidlertid *også* kunne anses for berettiget, selvom behandlingen i øvrigt er lovlig. Dette vil være tilfældet, hvis den registrerede har anført tungtvejende grunde til støtte for, at behandlingen pga. den registreredes særlige, individuelle situation ikke bør finde sted. Den dataansvarlige skal altså foretage en konkret vurdering af, om der foreligger sådanne særlige omstændigheder omkring netop denne registrerede person, at behand-

[456] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.5.3. i de almindelige bemærkninger.
[457] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.1.

lingen af oplysninger om den pågældende bør indskrænkes eller helt indstilles. Dette vil efter omstændighederne f.eks. kunne være tilfældet for en medarbejder i en myndighed eller virksomhed, som pga. chikane fra en tidligere ægtefælle ikke ønsker sit navn anført i en medarbejderfortegnelse på en hjemmeside på internettet.[458]

Det fremgår af bemærkningerne til persondataloven, at i tilfælde af, at en behandling ikke er lovlig skal den dataansvarlige i øvrigt ophøre med behandlingen, *uanset* om der gøres indsigelse herimod, jf. § 5, stk. 4, 2. pkt. Det fremgår endvidere af bemærkningerne til loven, at bestemmelsen imidlertid også indebærer, at den dataansvarlige – hvis der gøres indsigelse – efter omstændighederne skal ophøre med en behandling, som i øvrigt er lovlig. En indsigelse vil også kunne anses for berettiget, selvom behandlingen i øvrigt er lovlig.[459]

Det fremgår derudover af bemærkningerne til persondataloven, at i en række tilfælde forudsættes det, at indsigelsen ikke skal tages til følge. Det gælder bl.a. tilfælde, hvor behandlingen af oplysninger om den registrerede sker i statistisk eller videnskabeligt øjemed eller er foreskrevet i lovgivningen. Som eksempel herpå kan nævnes domstolenes behandling af oplysninger i forbindelse med udøvelse af judiciel virksomhed efter reglerne i retsplejeloven. Det er den dataansvarlige, som træffer afgørelse om berettigelsen af den registreredes indsigelse, og afgørelsen vil kunne indbringes for Datatilsynet.[460]

Det fremgår endelig af bemærkningerne til persondataloven, at den indsigelsesret, der efter stk. 1 tilkommer den registrerede, har den virkning, at en forvaltningsmyndigheds beslutning om, hvorvidt indsigelsen skal imødekommes, har karakter af en »afgørelse« efter forvaltningsloven. Det indebærer, at den pågældende myndighed skal overholde forvaltningslovens regler om begrundelse, klagevejledning mv.

Det bemærkes, at også i de tilfælde, hvor en behandling er lovlig med hjemmel i en særlov, vil indsigelsesretten efter persondatalovens § 35 kunne finde anvendelse.

Fra praksis kan nævnes en sag vedrørende sletning af profil og indlæg på et debatforum, hvor Datatilsynet udtalte, at tilsynet umiddelbart ikke fandt, at der i sagen var spørgsmål i relation til persondatalovens behandlingsregler, da den registrerede selv havde gjort oplysningerne tilgængelige på den dataansvarliges hjemmeside. Efter Datatilsynets opfattelse ville en indsigelse imidlertid også kunne anses for berettiget, selvom behandlingen i øvrigt

[458] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.1.
[459] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 35.
[460] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 35.

er lovlig. Det ville være tilfældet, hvis vægtige grunde, der vedrører den registreredes særlige situation, talte for, at indsigelsen skulle imødekommes. På denne baggrund fandt Datatilsynet, at den dataansvarlige ikke var berettiget til at opretholde den registreredes profil og indlæg i en form, der kunne henføres til den registrerede som person, efter at den registrerede havde fremsat ønske om sletning.[461]

I en sag vedrørende sletning hos et kreditoplysningsbureau, klagede en privat person over at være blevet registreret i et kreditoplysningsbureau. Den registrerede henviste til, at grundlaget for registreringen af ham var et falsk dokument, ligesom den registreredes ægtefælle havde givet møde i fogedretten i henhold til en falsk fuldmagt. Oplysningerne i sagen pegede i retning af, at den registreredes indsigelser var korrekte. Datatilsynet fandt ikke grundlag for at kritisere registreringen, men fandt, at den registrerede i forbindelse med henvendelsen til tilsynet havde anført så tungtvejende grunde, at hans indsigelse burde imødekommes efter persondatalovens § 35.[462]

Endelig kan nævnes en sag vedrørende en klage over offentliggørelse af navn og adresse på en kommunes hjemmeside, hvor Datatilsynet fandt, at den registrerede i forbindelse med henvendelsen til tilsynet havde anført så tungtvejende grunde, at indsigelsen om fjernelse af oplysningerne burde imødekommes. Der var tale om oplysninger om en læges navn og adresse, som fremgik af en kommunes behandling i forbindelse med en lokalplan. Lægen ønskede ikke, at oplysningerne blev behandlet, idet han i medfør af sit job som læge tidligere havde været udsat for indbrud fra narkomaner. Selvom behandlingen kunne ske efter persondatalovens § 6, stk. 1, nr. 5, 6 og 7, var indsigelsen berettiget, idet der forelå tungtvejende grunde hertil.[463]

4.11.2.2. Persondatalovens § 36

Der er i persondatalovens § 36 fastsat særlige regler for de registreredes ret til indsigelse ved markedsføring. Bestemmelsen er baseret på artikel 14, litra b, i databeskyttelsesdirektivet, hvoraf det blandt andet fremgår, at medlemsstaterne skal indrømme den registrerede ret til efter anmodning og uden udgifter at modsætte sig en behandling af personoplysninger, der vedrører den pågældende, og som den dataansvarlige agter at foretage med henblik på markedsføring.

[461] Sag vedrørende sletning af profil og indlæg på et debatforum, Datatilsynets brev af 19. november 2009.
[462] Sag vedrørende sletning i kreditoplysningsbureau grundet tungtvejende individuel indsigelse, Datatilsynets j.nr. 2013-221-0171.
[463] Sag vedrørende klage over offentliggørelse af navn og adresse på kommunes hjemmes, Datatilsynets j.nr. 2004-313-0247.

Det følger endvidere af artikel 14, litra b, at medlemsstaterne skal træffe de nødvendige foranstaltninger til at sikre, at de registrerede er bekendt med den i litra b, første afsnit, omhandlede ret.

Det følger således af persondatalovens § 36, stk. 1, at fremsætter en forbruger indsigelse herimod, må en virksomhed ikke videregive oplysninger om den pågældende til en anden virksomhed med henblik på markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed.

Datatilsynet anfører i vejledning om registreredes rettigheder, at der er tale om en ubetinget indsigelsesret, som kan gøres gældende direkte over for den dataansvarlige virksomhed på et hvilket som helst tidspunkt. Indsigelsen kan omfatte al videregivelse eller begrænses til videregivelse til bestemte virksomheder eller kategorier af virksomheder. Hvis intet andet angives i indsigelsen, må den almindeligvis forstås som en generel indsigelse mod al videregivelse og anvendelse på vegne af andre, der foretages med henblik på markedsføring.[464]

Der er ingen formkrav til indsigelsen, og den kan derfor fremsættes såvel mundtligt som skriftligt eller via elektronisk post. Virksomheden bør notere og gemme modtagne indsigelser, ligesom den bør tjekke sine optegnelser hver gang den ønsker at videregive kundeoplysninger til brug for markedsføring.[465]

Reglerne i § 36 gælder ikke kun i den situation, hvor en virksomhed ønsker at videregive oplysninger om en forbruger til en anden virksomhed med henblik på markedsføring. Reglerne gælder også, hvis virksomheden i stedet for at videregive oplysningerne anvender dem på vegne af en anden virksomhed med henblik på markedsføring. Denne situation vil typisk foreligge, når en virksomhed fra en anden virksomhed modtager markedsføringsmateriale i form af »direct mails« eller lignende og derefter udsender materialet til sine egne kunder, eventuelt selektivt ud fra de oplysninger om de enkelte kunders forbrugsvaner og -mønstre, som virksomheden er i besiddelse af.[466]

[464] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.2.2.
[465] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.2.2.
[466] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.2.

Det er kun registrerede personer, der er forbrugere, som er beskyttet af reglerne om indsigelsesret i § 36. Uden for begrebet »forbrugere« falder oplysninger om leverandører, andre forretningsforbindelser eller erhvervsdrivende.[467]

4.11.2.3. Oplysningspligt i forbindelse med indsigelsesret

I dansk ret er der ikke en udtrykkelig bestemmelse, som fastslår, at den registrerede *skal* gøres opmærksom på indsigelsesretten. Det kan dog ikke udelukkes, at denne retstilstand ville kunne blive resultatet efter en konkret vurdering efter gældende ret. Efter gældende ret ville et sådant krav om en oplysningspligt i forbindelse med indsigelsesret kunne følge af oplysningspligten for den dataansvarlige efter persondatalovens §§ 28 og 29 samt god databehandlingsskik.

Datatilsynet anfører således i tilsynets vejledning om registreredes rettigheder, at opregningerne i persondatalovens § 28, stk. 1, nr. 3, litra a-c, og § 29, stk. 1, nr. 3, litra a-c, ikke er udtømmende, hvorfor det efter omstændighederne vil kunne påhvile den dataansvarlige en pligt til at give den registrerede anden information end de oplysninger, som følger af bestemmelsen. Datatilsynet anfører endvidere, at vurderingen af, hvorvidt der skal gives den registrerede yderligere information beror på en konkret vurdering af, om dette er nødvendigt for, at den registrerede kan varetage sine interesser i det enkelte tilfælde.[468]

4.11.3. Databeskyttelsesforordningen

Det fremgår af Kommissionens forslag fra 2012 til databeskyttelsesforordningen, at den nuværende artikel 21 er baseret på artikel 14 i databeskyttelsesdirektivet med visse ændringer, herunder med hensyn til bevisbyrden og anvendelsen på direkte markedsføring.[469]

4.11.3.1. Databeskyttelsesforordningens artikel 21, stk. 1 – indsigelsesret i forbindelse med behandling baseret på artikel 6, stk. 1, litra e eller f

Det fremgår af databeskyttelsesforordningens artikel 21, stk. 1, at den registrerede til enhver tid har ret til af grunde, der vedrører den pågældendes særlige situation, at gøre indsigelse mod behandling af sine personoplysninger baseret på artikel 6, stk. 1, litra e eller f, herunder profilering baseret på disse bestemmelser. Den dataansvarlige må ikke længere behandle personoplysningerne, medmindre den dataansvarlige påviser vægtige legitime grunde til behandlingen, der går forud for registreredes interesser, rettigheder og frihedsrettigheder, eller behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.

[467] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 4.2.
[468] Vejledning nr. 126 af 10. juli 2000, om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, afsnit 2.1.3 og 2.2.3.
[469] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig).

Det fremgår af præambelbetragtning nr. 69, at hvis personoplysninger kan behandles lovligt, fordi behandling er nødvendig for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, eller af hensyn til en dataansvarligs eller en tredjemands legitime interesse, bør en registreret ikke desto mindre have ret til at gøre indsigelse mod behandling af personoplysninger på baggrund af den pågældendes særlige situation. Det bør være op til den dataansvarlige at påvise, at dennes vægtige legitime interesse har forrang for den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder.

For så vidt angår ordlyden i forordningens artikel 21, stk. 1, i forhold til persondatalovens § 35, og databeskyttelsesdirektivets artikel 14, litra a, ses bestemmelserne at indeholde det samme princip om den registreredes ret til indsigelse.

Som anført ovenfor har persondatalovens § 35 et bredere anvendelsesområde end databeskyttelsesdirektivets artikel 14, litra a, idet det efter persondataloven vil være behandling baseret på alle lovens behandlingshjemler, som den registrerede kan gøre indsigelse omkring og ikke blot behandling efter databeskyttelsesdirektivets artikel 7, litra e og f.

Databeskyttelsesforordningens artikel 21, stk. 1, indeholder – ligesom databeskyttelsesdirektivet – en begrænsning af bestemmelsens anvendelsesområde, således at det kun er i forbindelse med behandling af personoplysninger efter artikel 6, stk. 1, litra e og f, at der kan gøres indsigelse efter bestemmelsen.

Derudover er muligheden i direktivets artikel 14, litra a, for at fastsætte nationale særregler ikke videreført i databeskyttelsesforordningen.

Indsigelsesretten efter databeskyttelsesforordningen har således et mere snævert anvendelsesområde end den indsigelsesret, som følger af persondatalovens § 35.

Artikel 21 i databeskyttelsesforordningen må fortolkes i overensstemmelse med den forståelse, som Registerudvalget havde af den oprindeligt foreslåede § 35 til persondataloven – baseret på artikel 14, litra a, i databeskyttelsesdirektivet – som i vidt omfang er i overensstemmelse med artikel 21 i databeskyttelsesforordningen. Registerudvalgets betragtninger i betænkning nr. 1345, vil derfor kunne benyttes som fortolkningsbidrag i forhold til forordningens artikel 21.

På baggrund af præambelbetragtning nr. 69, følger det, at bestemmelsen alene omfatter de tilfælde, hvor behandling af oplysninger er lovlig efter bestemmelserne i forordningen. I

disse tilfælde skal der efter bestemmelsen gives den registrerede ret til under nærmere angivne betingelser at gøre indsigelse mod behandlingen af oplysninger.

Dette følger også af princippet i databeskyttelsesforordningens artikel 5, stk. 1, litra d, hvoraf det fremgår, at personoplysninger skal være korrekte og om nødvendigt ajourførte. Der skal således tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«).

Databeskyttelsesforordningens artikel 21, stk. 1, bevirker, at den registrerede ikke kan gøre indsigelse, når der sker lovlig behandling med hjemmel i forordningens artikel 6, stk. 1, litra a-d. Det må endvidere også være tilfældet for lovlig behandling med hjemmel i forordningens artikel 9 og 10, medmindre der gøres indsigelse efter artikel 21, stk. 6.

Bestemmelsen er modsat indsat med henblik på den situation, at en registreret er i en særlig situation, som gør, at den registrerede kan have en indsigelsesret omkring en ellers lovlig behandling. I sådanne tilfælde vil det således påhvile den dataansvarlige at løfte bevisbyrden for, at behandlingen kan fortsætte, men dog kun i de tilfælde, hvor behandlingen sker på grundlag af forordningens artikel 6, stk. 1, litra e og f. Det er i den forbindelse vigtigt at holde sig for øje, at den registrerede altid kan kræve, at behandling, der ikke er i overensstemmelse med forordningens bestemmelser, stoppes, herunder bl.a. efter artikel 5.

Som anført følger det af gældende ret, at den dataansvarlige skal foretage en konkret vurdering af, om der foreligger sådanne særlige omstændigheder omkring netop denne registrerede person, at behandlingen af oplysninger om den pågældende bør indskrænkes eller helt indstilles. Efter ordlyden af forordningens artikel 21, stk. 1, vil der også efter denne bestemmelse skulle foretages en konkret afvejning af hensynet til den pågældende registreredes særlige situation oven for legitime grunde til behandlingen, som går forud for den registreredes interesser.

Bestemmelsen i forordningens artikel 21, stk. 1, indeholder således fortolkningsbidrag til, hvad den dataansvarlige skal tillægge betydning i vurderingen af, hvorvidt der fortsat kan ske behandling af personoplysningerne.

Som efter gældende ret vil vurderingen af, hvorvidt indsigelsen skal imødekommes, for offentlige myndigheder have karakter af en »afgørelse« efter forvaltningsloven. Det indebærer, at den pågældende myndighed skal overholde forvaltningslovens regler om begrundelse, klagevejledning mv.

Da det fremgår af databeskyttelsesforordningens artikel 6, stk. 1, litra f, 2. afsnit, at første afsnit, litra f, ikke gælder for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver, vil indsigelsesretten efter forordningens artikel 21, stk. 1, vedrørende artikel 6, stk. 1, litra f, derfor som udgangspunkt ikke være relevant for offentlige myndigheder.

Det fremgår af forordningens artikel 21, stk. 1, at det er den dataansvarlige, som skal *påvise* vægtige legitime grunde til behandlingen, der går forud for registreredes interesser, rettigheder og frihedsrettigheder, eller behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.

Det følger endvidere af databeskyttelsesforordningens artikel 17, stk. 1, litra c, at den registrerede har ret til at få personoplysninger om sig selv slettet af den dataansvarlige uden unødig forsinkelse, og den dataansvarlige har pligt til at slette personoplysninger uden unødig forsinkelse, hvis den registrerede gør indsigelse mod behandlingen i henhold til artikel 21, stk. 1, og der ikke foreligger legitime grunde til behandlingen, som går forud for indsigelsen, eller den registrerede gør indsigelse mod behandlingen i medfør af artikel 21, stk. 2.

Som anført følger det af gældende ret, at den dataansvarlige – hvis der gøres indsigelse – efter omstændighederne skal ophøre med en behandling, som i øvrigt er lovlig. Det er endvidere den dataansvarlige, som træffer afgørelse om en indsigelse fra den registrerede.

På denne baggrund må det antages, at det allerede følger af reglerne i persondataloven, at det er den dataansvarlige, som skal påvise, at behandlingen af oplysninger kan fortsætte efter en indsigelse. I hvert fald fastlægges det nu med databeskyttelsesforordningen, at det er den dataansvarlige, som skal påvise vægtige legitime grunde til behandlingen, førend behandlingen kan fortsætte.

Princippet i databeskyttelsesforordningens artikel 21, stk. 1, ses ud fra en fortolkning af bestemmelsens ordlyd sammenholdt med, hvad der fremgår af præambelbetragtning nr. 69, overordnet set ikke at være en ændring af gældende ret, idet indsigelsesretten også følger af gældende ret. Der er dog den begrænsning i forhold til gældende ret, at der efter artikel 21, stk. 1, kun kan gøres indsigelse i forbindelse med de situationer, hvor behandlingen sker med hjemmel i forordningens artikel 6, stk. 1, litra e og f, og dermed ikke forordningens andre behandlingshjemler.

4.11.3.2. Databeskyttelsesforordningens artikel 21, stk. 2 og 3 – indsigelsesret i forbindelse med direkte markedsføring

Det fremgår af forordningens artikel 21, stk. 2, at hvis personoplysninger behandles med henblik på direkte markedsføring, har den registrerede til enhver tid ret til at gøre indsigelse mod behandling af sine personoplysninger til sådan markedsføring, herunder at gøre indsigelse mod profilering, i det omfang den vedrører direkte markedsføring.

Det fremgår endvidere af forordningens artikel 21, stk. 3, at hvis den registrerede gør indsigelse mod behandling med henblik på direkte markedsføring, må personoplysningerne ikke længere behandles til dette formål.

Det fremgår af præambelbetragtning nr. 70, at hvis personoplysninger behandles med henblik på direkte markedsføring, bør den registrerede til enhver tid have ret til gratis at gøre indsigelse mod en sådan behandling, herunder profilering, i det omfang den vedrører direkte marketing, uanset om det drejer sig om indledende behandling eller viderebehandling. Den registrerede bør udtrykkelig gøres opmærksom på denne ret, og oplysningerne bør gives klart og adskilt fra alle andre oplysninger.

Ved direkte markedsføring må skulle forstås markedsføring, som er rettet direkte mod en bestemt person.

Bestemmelserne i databeskyttelsesforordningens artikel 21, stk. 2 og 3, ses ud fra en fortolkning af bestemmelsens ordlyd sammenholdt med, hvad der fremgår af præambelbetragtning nr. 70, overordnet ikke at være en ændring af gældende ret, idet indsigelsesretten i forbindelse med direkte markedsføring også følger af gældende ret. Der er dog den begrænsning i forhold til gældende ret, at der efter artikel 21, stk. 2 og 3, kun kan gøres indsigelse i forbindelse med de situationer, hvor der er tale om direkte markedsføring.

Endvidere fremhæves det i forordningen nu udtrykkeligt i artikel 21, stk. 3, at behandling med henblik på direkte markedsføring (herunder for profilering, i det omfang den vedrører direkte markedsføring) ikke længere må ske, hvis den registrerede gør indsigelse herimod.

Profilering

Det fremgår af forordningens artikel 21, stk. 1, at den registrerede også har ret til at gøre indsigelse mod behandling af sine personoplysninger baseret på *profilering* efter artikel 6, stk. 1, litra e og f.

Det fremgår endvidere af forordningens artikel 21, stk. 2, at den registrerede også har ret til at gøre indsigelse mod *profilering, i det omfang den vedrører direkte markedsføring.*

Profilering defineres i forordningens artikel 4, nr. 4, hvoraf det fremgår, at profilering defineres som enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser.

Det fremhæves således af forordningens artikel 21, stk. 1 og 2, at den også finder anvendelse i forbindelse med profilering.

4.11.3.3. Databeskyttelsesforordningens artikel 21, stk. 4 – oplysning om indsigelsesretten
Det fremgår af databeskyttelsesforordningen artikel 21, stk. 4, at senest på tidspunktet for den *første kommunikation* med den registrerede *skal* denne udtrykkeligt gøres opmærksom på den ret, der er omhandlet i stk. 1 og 2, og oplysninger herom skal meddeles klart og adskilt fra alle andre oplysninger.

Efter gældende ret er der som nævnt ovenfor ikke et eksplicit krav om en sådan oplysningspligt i forbindelse med indsigelsesretten efter persondatalovens § 35, men det kan ikke udelukkes, at dette efter en konkret vurdering kunne være retstilstanden i en given situation.

Databeskyttelsesforordningens indeholder i artikel 13, stk. 2, litra b, om oplysningspligt ved indsamling af personoplysninger hos den registrerede og i artikel 14, stk. 2, litra c, om oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede, bestemmelser, hvoraf det følger, at den dataansvarlige skal give den registrerede oplysning om bl.a. retten til at gøre indsigelse mod behandling, der er nødvendige for at sikre en rimelig og gennemsigtig behandling.

Forordningens artikel 21, stk. 4, regulerer yderligere den oplysningspligt, som skal opfyldes omkring den indsigelsesret, som følger af samme bestemmelses stk. 1 og 2, herunder formkravene til meddelelsen i den forbindelse.

I forordningens artikel 21, stk. 4, præciseres det således, at meddelelsen skal gives senest på tidspunktet for den første kommunikation med den registrerede og endvidere, at den registrerede *udtrykkeligt* skal gøres opmærksom på indsigelsesretten.

Dette krav om udtrykkelighed må skulle forstås som udtrykkelighed i forbindelse med et samtykke til behandling af følsomme oplysninger efter forordningens artikel 9, stk. 2, litra a, hvorfor der heri må antages at ligge et krav om, at meddelelsen skal være *klar og utvety-*

dig. Kravet om udtrykkelighed må antages at føre til, at der ikke er mulighed for, at den dataansvarlige stiltiende eller indirekte gør den registrerede opmærksom på indsigelsesretten efter artikel 21, stk. 1 og 2.

Derudover følger det af forordningens artikel 21, stk. 4, at meddelelsen skal gives klart og adskilt fra alle andre oplysninger.

4.11.3.4. Databeskyttelsesforordningens artikel 21, stk. 5 – indsigelse gennem automatiske midler ved brug af tekniske specifikationer

Det fremgår af databeskyttelsesforordningens artikel 21, stk. 5, at i forbindelse med anvendelse af informationssamfundstjenester og uanset direktiv 2002/58/EF kan den registrerede udøve sin ret til indsigelse gennem automatiske midler ved brug af tekniske specifikationer.

I forordningens artikel 4, nr. 25, er informationssamfundstjeneste defineret som en tjeneste som defineret i artikel 1, stk. 1, litra b, i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 (informationsproceduredirektivet).

Af dette direktivs artikel 1, stk. 1, litra b, fremgår, at der ved begrebet "tjeneste" forstås enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager. For nærmere herom henvises til afsnit 2.3. om definitioner.

Med denne bestemmelse fastslår forordningen, at den registrerede har ret til i forbindelse med informationssamfundstjenester, som eksempelvis kan være Facebook, Instagram, Snapchat, Netflix samt almindelige hjemmesider og internetportaler, der opfylder de ovennævnte betingelser, at gøre indsigelse gennem automatiske midler ved brug af tekniske specifikationer.

En sådan ret fremgår ikke direkte af gældende ret, hvorfor der er tale om en nyskabelse, hvorefter den registrerede har krav på at gøre indsigelse gældende i den form, som bestemmelsen anfører i forbindelse med anvendelse af informationssamfundstjenester.

4.11.3.5. Databeskyttelsesforordningens artikel 21, stk. 6 – indsigelse i forbindelse med videnskabelige eller historiske forskningsformål eller statistiske formål i henhold til artikel 89, stk. 1

Det fremgår af databeskyttelsesforordningens artikel 21, stk. 6, at hvis personoplysninger behandles med henblik på videnskabelige eller historiske forskningsformål eller statistiske formål i henhold til artikel 89, stk. 1, har den registrerede ret til af grunde, der vedrører den

pågældendes særlige situation at gøre indsigelse mod behandling af personoplysninger vedrørende den pågældende, medmindre behandlingen er nødvendig for at udføre en opgave i samfundets interesse.

Denne bestemmelse fastslår således, at den registrerede også har en indsigelsesret i forbindelse med den behandling, som sker i overensstemmelse med forordningens artikel 89, stk. 1, og at den registrerede også her kan gøre indsigelse i forhold til dennes særlige situation. Dog følger det af bestemmelsen, at en sådan indsigelse ikke vil være berettiget, såfremt behandlingen er nødvendig for at udføre en opgave i samfundets interesse. Efter denne bestemmelse skal der således – ligesom efter forordningens artikel 21, stk. 1 – ske en afvejning af hensynet til den registreredes særlige situation ovenfor behandlingens nødvendighed for at udføre en opgave i samfundets interesse.

Efter forordningens artikel 21, stk. 6, vil den registrerede kunne gøre indsigelse mod behandling med henblik på videnskabelige eller historiske forskningsformål eller statistiske formål, medmindre behandlingen hertil er nødvendig for at udføre en *opgave i samfundets interesse*. Et sådan afvejning af, at behandling alligevel kan finde sted, såfremt den er i samfundets interesse, må allerede antages at være en del af gældende ret, da der netop efter persondatalovens § 35 skal foretages en konkret afvejning.

Bestemmelserne i databeskyttelsesforordningens artikel 21, stk. 6, ses ud fra en fortolkning af bestemmelsens ordlyd, ikke at være en ændring af, hvad der allerede følger af gældende ret – dog bliver det i bestemmelsen fremhævet, at den behandling, som sker med henblik på videnskabelige eller historiske forskningsformål eller statistiske formål i henhold til artikel 89, stk. 1, skal være nødvendig for at udføre en opgave i samfundets interesse, hvis indsigelsen ikke skal accepteres.

4.11.4. Overvejelser

Princippet i databeskyttelsesforordningens artikel 21 er i et vist omfang en videreførelse af gældende ret – dog vil den registrerede efter bestemmelsen i artikel 21, stk. 1, kun kunne gøre indsigelse i de tilfælde, hvor behandlingen af oplysninger sker med hjemmel i forordningens artikel 6, stk. 1, litra e og f. Modsat efter gældende ret, vil det derfor kun være i forbindelse med behandling af almindelige personoplysninger, som sker på baggrund af udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse eller for at forfølge en legitim interesse, at den registrerede har ret til at gøre indsigelse.

Det er i den forbindelse vigtigt at holde sig for øje, at bestemmelsen om retten til indsigelse er indsat med henblik på den situation, at den registrerede er i en særlig situation, som gør,

at den registrerede kan have en indsigelse i forbindelse med en ellers lovlig behandling. Retten til indsigelse forudsætter således ikke, at der sker behandling i strid med forordningens bestemmelser. Den registrerede vil efter databeskyttelsesforordningen – modsat efter gældende ret – ikke kunne gøre indsigelse i de tilfælde, hvor behandlingen af oplysninger sker med hjemmel i eksempelvis forordningens artikel 6, stk. 1, litra a-d, eller artikel 9 og 10, medmindre der gøres indsigelse efter artikel 21, stk. 6.

Databeskyttelsesforordningens artikel 21, stk. 2 og 3, er overordnet en videreførelse af gældende ret, men det bemærkes dog, at efter artikel 21, stk. 2 og 3, kan der kun gøres indsigelse i forbindelse med de situationer, hvor der er tale om direkte markedsføring.

Vedrørende forordningens artikel 21, stk. 4, om oplysning om indsigelsesret efter artikel 21, stk. 1 og 2, er der tale om et nyt krav til den dataansvarlige. Det ses således ikke ud fra praksis i gældende dansk ret at være blevet fastslået, at der helt generelt gælder sådanne krav. Det kan dog ikke udelukkes, at denne retstilstand ville kunne blive resultatet i en konkret sag efter gældende ret. Ikke desto mindre, så fastlægger forordningen klart denne oplysningspligt i forbindelse med indsigelsesretten, hvorfor den dataansvarlige i hvert fald, når forordningen finder anvendelse fra den 25. maj 2018, vil skulle overholde kravene heri.

Databeskyttelsesforordningens artikel 21, stk. 5, fastslår i en, i forhold til gældende ret, ny bestemmelse, hvordan den registrerede rent praktisk har ret til at gøre indsigelse i forbindelse med indsigelse ved anvendelse af informationssamfundstjenester.

Endelig ses databeskyttelsesforordningens artikel 21, stk. 6, om indsigelsesret i forbindelse med behandling med henblik på videnskabelige eller historiske forskningsformål eller statistiske formål i henhold til artikel 89, stk. 1, ikke at være en ændring af, hvad der allerede følger af gældende ret – dog bliver det i bestemmelsen fremhævet, at behandlingen skal være nødvendig for at udføre en opgave i samfundets interesse.

4.12. Automatiske afgørelser, artikel 22

4.12.1. Præsentation

Persondatalovens § 39 vedrører den registreredes ret til ikke at være genstand for automatiske individuelle afgørelser.

Databeskyttelsesforordningen indeholder en tilsvarende bestemmelse i artikel 22, hvorefter den registrerede har ret til ikke at være genstand for en afgørelse, der alene er baseret på

automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.

4.12.2. Gældende ret

4.12.2.1. Persondatalovens § 39, stk. 1 (ret til ikke at være genstand for foranstaltninger baseret på automatiske individuelle afgørelser)

Det fremgår af persondatalovens § 39, at fremsætter en registreret person indsigelse herimod, kan den dataansvarlige ikke foranstalte, at den registrerede undergives afgørelser, der har retsvirkninger for eller i øvrigt berører den pågældende i væsentlig grad, og som alene er truffet på grundlag af elektronisk databehandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold.

Efter databeskyttelsesdirektivet artikel 15, stk. 1, følger det tilsvarende, at medlemsstaterne indrømmer enhver person ret til ikke at være undergivet afgørelser, der har retsvirkning for ham, eller som berører ham i væsentlig grad, og som alene er truffet på grundlag af edb-behandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold, såsom erhvervsevne, kreditværdighed, pålidelighed, adfærd osv.

Persondatalovens § 39 er fastsat på baggrund af muligheden herfor i direktivets artikel 15, stk. 1.

Registerudvalget udtalte i betænkning nr. 1345, at den ret til at gøre indsigelse, som følger af artikel 15, er ubetinget i den forstand, at de nævnte former for behandling af oplysninger ikke kan ske, hvis den registrerede gør indsigelse herimod.[470]

Registerudvalget anførte vedrørende forståelsen af persondatalovens § 39, at databeskyttelsesdirektivets artikel 15, stk. 1, efter sin ordlyd ikke er ganske klar, men at bestemmelsen måtte antages at skulle forstås således, at der alene påhviler medlemsstaterne en pligt til at give registrerede personer ret til at gøre indsigelse mod edb-behandlede individuelle afgørelser. Udvalget anførte dernæst, at en forpligtelse til helt at forbyde sådanne afgørelser således ikke kunne antages at følge af bestemmelsen. Udvalget bemærkede endvidere, at de lovudkast, som var udarbejdet af henholdsvis det norske og det svenske personregisterudvalg, også byggede på en ordning, hvorefter den registrerede har en indsigelsesret over for edb-behandlede afgørelser.[471]

Det fremgår af bemærkningerne til persondataloven, at der skal være tale om afgørelser, der kan gøres gældende over for den registrerede, og som har konsekvenser for den pågæl-

[470] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 317.
[471] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 319.

dende. Den omstændighed, at der f.eks. udsendes materiale af oplysende karakter til en række personer, der står opført på en edb-liste, vil ikke udgøre en afgørelse i den foreslåede bestemmelses forstand.[472]

Det fremgår endvidere af bemærkningerne, at der skal være tale om afgørelser, der *alene* er truffet på grundlag af en edb-behandling. Bestemmelsen omhandler dermed kun den situation, at der uden videre gøres brug af resultater, som et edb-system leverer. Edb må således efter bestemmelsen være en hjælp ved beslutningstagningen, hvorimod edb-behandling af oplysningerne ikke må udgøre det eneste grundlag for en beslutning, hvor den menneskelige vurdering bør spille ind. Som eksempel herpå anføres det, at en arbejdsgiver ikke må afvise en jobansøger på grundlag af resultatet af en psykoteknisk prøve, der alene behandles på edb, eller på baggrund af lister, som er udarbejdet under anvendelse af vurderingsprogrammel, og som på grundlag af en personlighedstest af jobansøgerne indeholder en bedømmelse af de pågældende, herunder en opstilling af dem i rangorden.[473]

Det fremgår endelig af bemærkningerne, at der skal være tale om edb-behandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold. Dette kan f.eks. være oplysninger om en persons erhvervsevne, kreditværdighed, pålidelighed, adfærd mv. Omfattet af bestemmelsen er behandlinger, hvorved der gøres brug af variabler, der fastsætter en typisk personlighedsprofil. Den omstændighed, at en person f.eks. ikke kan hæve et ønsket beløb i en pengeautomat, fordi der ikke er dækning for beløbet, falder uden for bestemmelsen. Tilsvarende gælder for så vidt angår told- og skattemyndighedernes edb-automatiserede ligningsarbejde.[474]

4.12.2.2. Persondatalovens § 39, stk. 2 (undtagelser)
Indsigelsesretten efter persondatalovens § 39, stk. 1, gælder ikke ubetinget.

Det følger således af persondatalovens § 39, stk. 2, nr. 1, at stk. 1 ikke gælder, hvis den pågældende afgørelse træffes som led i indgåelsen eller opfyldelsen af en aftale, såfremt den registreredes anmodning om indgåelse eller opfyldelse af aftalen er blevet efterkommet, eller der findes passende foranstaltninger til at beskytte den registreredes berettigede interesser.

[472] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 35, de specielle bemærkninger til § 39.
[473] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 35, de specielle bemærkninger til § 39.
[474] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 35, de specielle bemærkninger til § 39.

Det fremgår tilsvarende af databeskyttelsesdirektivets artikel 15, stk. 2, litra a, at uden, at dette berører de øvrige bestemmelser i direktivet, fastsætter medlemsstaterne bestemmelser om, at en person kan undergives en afgørelse af den art, der er omhandlet i artikel 15, stk. 1, når den pågældende afgørelse træffes som led i indgåelsen eller opfyldelsen af en kontrakt, såfremt den registreredes anmodning om indgåelse eller opfyldelse af kontrakten er blevet efterkommet, eller der findes passende foranstaltninger til at beskytte den registreredes legitime interesser, som f.eks. mulighed for denne til at gøre sit synspunkt gældende.

Det fremgår af bemærkningerne til persondataloven, at passende foranstaltninger bl.a. vil kunne følge af en lov, af anmeldelsesprocedurerne eller af interne foranstaltninger truffet af den dataansvarlige.[475]

Det følger endvidere af persondatalovens § 39, stk. 2, nr. 2, at stk. 1 ikke gælder, hvis den pågældende afgørelse er hjemlet i en lov, der indeholder bestemmelser til beskyttelse af den registreredes berettigede interesser.

Det fremgår tilsvarende af databeskyttelsesdirektivets artikel 15, stk. 2, litra b, at uden, at dette berører de øvrige bestemmelser i direktivet, fastsætter medlemsstaterne bestemmelser om, at en person kan undergives en afgørelse af den art, der er omhandlet i artikel 15, stk. 1, når den pågældende afgørelse er hjemlet i en lov, der indeholder bestemmelser til beskyttelse af den registreredes legitime interesser.

4.12.2.3.1. Persondatalovens § 39, stk. 3 (ret til oplysning)
Det fremgår af persondatalovens § 39, stk. 3, at den registrerede har ret til hos den dataansvarlige snarest muligt og uden ugrundet ophold at få at vide, hvilke beslutningsregler der ligger bag en afgørelse, som nævnt i stk. 1.

Det fremgår af bemærkningerne til persondataloven, at en betingelse for, at den registrerede har ret til den i bestemmelsen angivne information, er, at der over for den pågældende er truffet en edb-baseret afgørelse, som omhandlet i stk. 1. I givet fald påhviler det den dataansvarlige at oplyse den registrerede om, hvorledes det edb-system, som har været anvendt til behandlingen af oplysningerne, er nået frem til afgørelsen.[476]

Det fremgår endvidere af bemærkningerne, at den registreredes ret efter bestemmelsen dog ikke fører til, at den dataansvarlige er forpligtet til at udlevere oplysninger, som må anses

[475] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 35, de specielle bemærkninger til § 39.
[476] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 35, de specielle bemærkninger til § 39.

for at være forretningshemmeligheder, eller som er beskyttet efter den immaterielle lovgivning, herunder ophavsretsloven.[477]

4.12.2.3.2. Persondatalovens § 39, stk. 3, og henvisningen til lovens § 30 – (undtagelser til den registreredes ret til oplysning)
Det fremgår af persondatalovens § 39, stk. 3, at lovens § 30 finder tilsvarende anvendelse.

For nærmere herom henvises til afsnit 4.13. om begrænsninger af rettighederne, artikel 23.

4.12.3. Databeskyttelsesforordningen
Det fremgår af Kommissionens forslag fra 2012 til databeskyttelsesforordningen, at artikel 22 omhandler den registreredes ret til ikke at være genstand for foranstaltninger baseret på profilering. Kommissionen anfører således, at med ændringer og yderligere garantier er artikel 22 baseret på artikel 15, stk. 1, i databeskyttelsesdirektivet om edb-behandlede individuelle afgørelser, ligesom der tages hensyn til Europarådets anbefaling om profilering, jf. CM/Rec (2010)13.[478]

4.12.3.1. Databeskyttelsesforordningens artikel 22, stk. 1 (ret til ikke at være genstand for foranstaltninger baseret på automatiske individuelle afgørelser, herunder profilering)
Det fremgår af databeskyttelsesforordningens artikel 22, stk. 1, at den registrerede har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.

I databeskyttelsesforordningen er der en tilføjelse i forhold til ordlyden i databeskyttelsesdirektivet og persondataloven, hvorefter profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den registrerede, er direkte nævnt i bestemmelsen.

Profilering defineres i forordningens artikel 4, nr. 4, hvoraf det fremgår, at profilering defineres som enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser.

[477] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 35, de specielle bemærkninger til § 39.
[478] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig).

Det fremgår tillige af præambelbetragtning nr. 71, at behandling efter artikel 22 omfatter »profilering«, der består af enhver form for automatisk behandling af personoplysninger, der evaluerer de personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den registreredes *arbejdsindsats, økonomisk situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografiske position eller bevægelser*, når den har retsvirkning for den pågældende eller på tilsvarende vis betydeligt påvirker den pågældende.

Profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den registrerede, vil allerede efter gældende ret være en del af anvendelsesområdet i persondatalovens § 39 og direktivets artikel 15, men det er nu i hvert fald konkretiseret, hvad der i forordningens forstand skal forstås ved profilering, ligesom det tydeliggøres, at profilering er omfattet af bestemmelsens anvendelsesområde.

Det fremgår af databeskyttelsesdirektivet, at *medlemsstaterne indrømmer enhver person ret til ikke at være undergivet afgørelser* efter artikel 15.

Det fremgår tilsvarende af databeskyttelsesforordningens artikel 22, at *den registrerede har ret til ikke at være genstand for en afgørelse* efter artikel 22.

Registerudvalget anførte i betænkning nr. 1345, som anført ovenfor vedrørende forståelsen af direktivets artikel 15, at selvom bestemmelsen ikke er ganske klar, finder udvalget dog, at bestemmelsen må antages at skulle forstås således, at der alene påhviler medlemsstaterne en pligt til at give registrerede personer ret til at gøre indsigelse mod edb-behandlede individuelle afgørelser. En forpligtelse til helt at forbyde sådanne afgørelser kan således ikke antages at følge af bestemmelsen.

Det samme ses at være tilfældet med databeskyttelsesforordningen, idet bestemmelsen som anført stort set har samme ordlyd som direktivet, og da der heller ikke ses at fremgå et direkte forbud mod automatiske individuelle afgørelser. Forordningens artikel 22, vil derfor ligesom efter persondatalovens § 39 – som er fastsat på baggrund af direktivets artikel 15 – skulle ses som en indsigelsesret for den registrerede.

Det fremgår af databeskyttelsesdirektivet samt persondataloven, at der skal være tale om afgørelser, som *i væsentlig grad berører den registrerede*.

I databeskyttelsesforordningen tales der om en afgørelse, der *betydeligt påvirker den registrerede*.

Efter en ordlydsfortolkning må der være samme forståelse af denne ordlyd, hvorfor denne del af bestemmelsen skal forstås i overensstemmelse med gældende ret. Det betyder eksempelvis, at der ligesom efter gældende ret skal være tale om afgørelser, der kan gøres gældende over for den registrerede, og som har konsekvenser for den pågældende. Den omstændighed, at der f.eks. udsendes materiale af oplysende karakter til en række personer, der står opført på en liste, vil ikke udgøre en afgørelse i artikel 22's forstand, idet der ikke træffes en afgørelse, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende. Eksempelvis vil markedsføring, i hvert fald af generel karakter, endvidere ikke være omfattet af bestemmelsen, idet der heller ikke i den forbindelse træffes en afgørelse i artikel 22's forstand.

Persondatalovens § 39 omhandler en afgørelse, *som alene er truffet på grundlag af elektronisk databehandling af oplysninge*r, mens databeskyttelsesdirektivet omhandler en afgørelse, *som alene er truffet på grundlag af edb-behandling af oplysninger*.

Efter databeskyttelsesforordningen omhandler artikel 22 en afgørelse, *der alene er baseret på automatisk behandling*.

Anvendelsesområdet for disse behandlinger ses at være det samme.

Præambelbetragtning nr. 71 indeholder som fortolkningsbidrag til, hvad der vil være en automatisk individuel afgørelse omfattet af artikel 22, at det kan være et automatisk afslag på en onlineansøgning om kredit eller e-rekrutteringsprocedurer uden nogen menneskelig indgriben.

Det fremgår ikke direkte af forordningen, at der skal være tale om oplysninger, *der er bestemt til at vurdere bestemte personlige forhold*, som det er tilfældet med persondatalovens § 39 og databeskyttelsesdirektivets artikel 15.

Det fremgår dog af præambelbetragtning nr. 71 til forordningen, at den registrerede bør have ret til ikke at blive gjort til genstand for en afgørelse, der kan omfatte en foranstaltning, som evaluerer personlige forhold vedrørende vedkommende, og som alene bygger på automatisk behandling og som har retsvirkning eller som på tilsvarende vis betydeligt påvirker den pågældende, såsom et automatisk afslag på en onlineansøgning om kredit eller e-rekrutteringsprocedurer uden nogen menneskelig indgriben.

Det fremgår i den forbindelse af forordningens artikel 4, nr. 4, at profilering er: enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at *evaluere bestemte personlige forhold* vedrørende en fysisk person, navnlig for

at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser.

Derudover er overskriften til artikel 22 automatiske individuelle afgørelser, hvilket også støtter det faktum, at afgørelsen skal vedrøre personlige forhold.

Anvendelsesområdet for disse behandlinger ses således ligeledes at være identisk med gældende ret.

Det er vigtigt at holde sig for øje, at den behandling, som omtales i artikel 22, er den automatiske behandling, hvor netop personlige forhold evalueres. Der vil således ikke være tale om en afgørelse i artikel 22's forstand, såfremt den afgørelse, der træffes, sker ved en rent matematisk udregning ud fra de givne faktuelle forudsætninger, uden at der dermed sker en evaluering af personlige forhold vedrørende vedkommende. Den omstændighed, at en person f.eks. ikke kan hæve et beløb i en pengeautomat, fordi der ikke er dækning for beløbet, falder eksempelvis uden for bestemmelsen.

Omvendt er det dog vigtigt at være opmærksom på, at artikel 22, stk. 1, netop regulerer de tilfælde, hvor behandling af personoplysninger sker automatisk (uden menneskelig indblanding) i et IT-system, herunder eksempelvis på baggrund af en eller anden form for matematisk eller statistisk procedure.

Det nævnte eksempel i præambelbetragtning nr. 71 med et automatisk afslag på en onlineansøgning om kredit eller e-rekrutteringsprocedurer uden nogen menneskelig indgriben viser således, at det kan være en automatisk afgørelse i artikel 22's forstand, også selvom der kun behandles oplysninger om vedkommendes personlige forhold i mere begrænset omfang.

Et eksempel på en automatisk afgørelse i artikel 22's forstand vil f.eks. kunne være, når et forsikringsselskab træffer automatisk afgørelse (uden menneskelig indblanding) om, at en 18-årig mand ikke kan tegne en bilforsikring. Her vil der være tale om en afgørelse, *der betydeligt påvirker den registrerede*, idet afgørelsen bevirker, at han ikke får en aftale med forsikringsselskabet.

Det vil endvidere eksempelvis være en automatisk afgørelse i artikel 22's forstand, hvis en bank træffer automatisk afgørelse (uden menneskelig indblanding) om, hvorvidt en person kan få bevilget et lån, idet en sådan afgørelse, *betydeligt påvirker den registrerede*.

Dernæst vil et forsikringsselskab automatiske afslag (uden menneskelig indblanding) på at dække en skade i henhold til en indgået forsikringsaftale med den registrerede ligeledes være en automatisk afgørelse i artikel 22's forstand, idet en sådan afgørelse vil *have retsvirkning* for forsikringstageren.

Endelig vil det i en ansættelsessammenhæng eksempelvis være en automatisk afgørelse i artikel 22's forstand, hvis arbejdsgiveren ud fra et automatiseret system på forhånd frasorterer en række ansøgere, eksempelvis på baggrund af deres karaktergennemsnit.

Det vil dog omvendt eksempelvis ikke være en afgørelse i artikel 22's forstand, hvis en kommune giver et barn automatisk afslag (uden menneskelig indblanding) på en plads i en daginstitution, udelukkende fordi barnets søskende går på en anden daginstitution, forudsat at der i et sådant afslag ikke er lagt vægt på en evaluering af personlige forhold vedrørende barnet, der har fået afslaget.

Bestemmelsen i forordningens artikel 22, stk. 1, svarer efter ordlyden til direktivets artikel 15, stk. 1, og persondatalovens § 39, stk. 1, hvorfor forordningens artikel 22, stk. 1, ses at svare til gældende ret.

4.12.3.2. Databeskyttelsesforordningens artikel 22, stk. 2 (undtagelser)
4.12.3.2.1. Databeskyttelsesforordningens artikel 22, stk. 2, litra a, om kontrakt, herunder artikel 22, stk. 3
Det fremgår af databeskyttelsesforordningens artikel 22, stk. 2, *litra a*, at bestemmelsens stk. 1 ikke finder anvendelse, hvis afgørelsen er *nødvendig* for indgåelse eller opfyldelse af en kontrakt mellem den registrerede og en dataansvarlig.

Det fremgår endvidere af forordningens artikel 22, stk. 3, at i de tilfælde, der er omhandlet i stk. 2, litra a, gennemfører den dataansvarlige passende foranstaltninger til at beskytte den registreredes rettigheder og frihedsrettigheder samt legitime interesser, i det mindste den registreredes ret til menneskelig indgriben fra den dataansvarliges side, til at fremkomme med sine synspunkter og til at bestride afgørelsen.

Det fremgår af præambelbetragtning nr. 71, at en sådan behandling under alle omstændigheder bør være omfattet af de fornødne garantier, herunder specifik underretning af den registrerede og retten til menneskelig indgriben, til at fremkomme med synspunkter, til at få en forklaring på den afgørelse, der er truffet efter en sådan evaluering, og til at bestride afgørelsen.

Dette bevirker, at en virksomhed, der lovligt træffer automatiske afgørelser efter artikel 22, stk. 2, litra a, skal sikre sig, at den registrerede har mulighed for at anmode om, at afgørelserne bliver genoptaget og dermed vurderet ved menneskelig indgriben af en medarbejder.

Bestemmelsen i forordningens artikel 22, stk. 2, litra a, sammenholdt med artikel 22, stk. 3, svarer efter ordlyden til direktivets artikel 15, stk. 2, litra a, og persondatalovens § 39, stk. 2, nr. 1, hvorfor disse bestemmelser svarer til gældende ret.

Det fremgår af ordlyden til forordningens artikel 22, stk. 2, litra a, at den automatiske afgørelse skal være *nødvendig* for indgåelse eller opfyldelse af en kontrakt mellem den registrerede og en dataansvarlig.

Kravet om "nødvendighed" knytter sig således til selve indgåelsen eller opfyldelsen af kontrakten. Kravet om "nødvendighed" må nærmere udfyldes i praksis.

Eksempelvis må det antages at være "nødvendigt", at den dataansvarlige træffer en automatisk afgørelse for at yde den registrerede den ydelse, som der er indgået aftale om, såfremt den dataansvarlige ellers skal bruge betydelige ressourcer på manuel behandling for at yde den registrerede ydelsen. Dette er dog under forudsætning af, at der er passende foranstaltninger, jf. forordningens artikel 22, stk. 3.

I sådanne situationer må virksomheder således have en vis mulighed for at tillægge eksempelvis ressourcemæssige hensyn betydning i vurderingen af, om den automatiske afgørelse er nødvendig.

4.12.3.2.2. Databeskyttelsesforordningens artikel 22, stk. 2, litra b, om national ret
Det fremgår endvidere af databeskyttelsesforordningens artikel 22, stk. 2, *litra b*, at bestemmelsens stk. 1 ikke finder anvendelse, hvis afgørelsen er hjemlet i EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt, og som også fastsætter passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser.

Det fremgår yderligere af præambelbetragtning 71, at afgørelser baseret på en sådan behandling, herunder profilering, bør være tilladt, når EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt, udtrykkelig tillader det, herunder med henblik på overvågning og forebyggelse af svig og skatteunddragelse i overensstemmelse med EU-institutionernes eller nationale tilsynsmyndigheders forskrifter, standarder og henstillinger og for at garantere sikkerheden og pålideligheden af en tjeneste, der ydes af den dataansvarlige.

Bestemmelsen i artikel 22, stk. 2, litra b, ses at svare til gældende ret.

Forordningens artikel 22 må på baggrund af artikel 22, stk. 2, litra b, forventes at få forholdsvis begrænset betydning for offentlige myndigheder, idet deres behandling af afgørelser, som muligvis kunne være omfattet af ordlyden i artikel 22, stk. 1, normalt vil være hjemlet i national ret.

Det må i den forbindelse bemærkes, at når det fremgår af artikel 22, stk. 2, litra b, at afgørelsen skal være hjemlet i national ret, kan det ikke antages også at være et krav, at den nationale lov specifikt regulerer, at afgørelsen skal ske uden menneskelig indblanding. Det må således antages, at når det i øvrigt er i overensstemmelse med national ret at beslutte, at afgørelser skal ske automatisk uden indblanding af en sagsbehandler, må man fortsat kunne træffe en sådan afgørelse.

Det bemærkes, at når det af undtagelsesbestemmelsen i artikel 22, stk. 2, litra b, fremgår, at den nationale ret skal fastsætte passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser, må det anses for en passende garanti, hvis borgeren f.eks. kan påklage den automatiske afgørelse til en overordnet myndighed, hvor klagesagen behandles ved menneskelig indblanding.

Det følger eksempelvis af SU-loven[479], at en ansøgning om SU alene kan ske gennem det digitale selvbetjeningssystem minSU. Afgørelsen om tildeling af SU (stipendium og lån) træffes automatisk på baggrund af den uddannelsessøgendes indskrivningsoplysninger (at den pågældende er optaget på en specifik uddannelsesinstitution og på en specifik uddannelse med en specifik støttetid), og støtten udbetales herefter til den uddannelsessøgendes Nemkonto efter oplysninger fra SKAT om beskatning.

Det fremgår af de almindelige bemærkninger til SU-loven, at effektiviseringsgevinsten ved selve digitaliseringen opnås ved, at de uddannelsessøgende selv indtaster ansøgningen i minSU, ved at selve SU-afgørelsen i højere grad automatiseres og ved effektivisering af vejledningen. Automatiseringen af SU-afgørelsen sker ved, at oplysninger, som ligger til grund for SU-afgørelsen, og som før digitaliseringen skulle fremgå af ansøgningen og indtastes i US2000, hentes fra andre offentlige myndigheders registre og fra uddannelsesinstitutionernes studieadministrative registre.[480]

[479] Bekendtgørelse nr. 39 af 15. januar 2014 af lov statens uddannelsesstøtte (SU-loven med senere ændringer).
[480] Forslag til lov nr. 75 fremsat 19. november 2008 om ændring af lov statens uddannelsesstøtte (SU-loven), de almindelige bemærkninger, afsnit 2.6.3.

Sådanne afgørelser vil som udgangspunkt kunne være omfattet af forordningens artikel 22, stk. 1.

Sådanne automatiske afgørelser vil således have hjemmel i SU-loven. Endvidere er der fastsat passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser, idet den uddannelsessøgende, hvis der ikke gives fuldt ud medhold, kan påklage afgørelsen til Ankenævnet for Statens Uddannelsesstøtte, som ikke træffer en automatisk afgørelse.

En sådan klagemulighed må anses som *et eksempel* på passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder i medfør af forordningens artikel 22, stk. 2, litra b.

Afgørelser efter SU-loven antages derfor under alle omstændigheder at kunne foretages i overensstemmelse med forordningens artikel 22, stk. 2, litra b.

Det følger endvidere som et eksempel af § 9 a i lov om inddrivelse af gæld til det offentlige[481], at modregning, der gennemføres af restanceinddrivelsesmyndigheden eller af told- og skatteforvaltningen som fordringshaver, kan ske uden partshøring af skyldneren og uden forudgående vurdering af dennes økonomiske forhold.

Det fremgår af bemærkningerne til lov om inddrivelse af gæld til det offentlige, at modregning i praksis sker i en automatiseret proces, der hviler på systemunderstøttelse.[482]

Det fremgår endvidere af bemærkningerne til lov om inddrivelse af gæld til det offentlige, at med henblik på at det hurtigt afklares, om eventuelle indsigelser fra skyldner i forhold til den gennemførte modregning giver anledning til, at hovedfordringen skal udbetales, vil der blive etableret en "fast track"-ordning, således at SKAT i de sager, hvor en skyldner påklager en modregning, som SKAT har gennemført som fordringshaver, inden for en frist på 14 dage skal afgive en udtalelse til Skatteankestyrelsen eller ændre afgørelsen, hvis SKAT i forbindelse med en genoptagelse af sagen finder anledning hertil.[483]

[481] Lov nr. 298 af 22. marts 2016 om ændring af lov om inddrivelse af gæld til det offentlige, lov om en børne- og ungeydelse og opkrævningsloven.
[482] Forslag til lov nr. L 122 fremsat 12. februar 2016 til lov om ændring af lov om inddrivelse af gæld til det offentlige, lov om en børne- og ungeydelse og opkrævningsloven, de almindelige bemærkninger, afsnit 2.4.
[483] Forslag til lov nr. L 122 fremsat 12. februar 2016 til lov om ændring af lov om inddrivelse af gæld til det offentlige, lov om en børne- og ungeydelse og opkrævningsloven, de almindelige bemærkninger, afsnit 2.4.

§ 9 a i lov om inddrivelse af gæld til det offentlige er et eksempel på, at SKAT har mulighed for at træffe afgørelser, der alene er baseret på automatisk behandling. En sådan afgørelse vil som udgangspunkt være omfattet af forordningens artikel 22, stk. 1.

De afgørelser, som SKAT træffer, har hjemmel i § 9 a i lov om inddrivelse af gæld til det offentlige. Endvidere er der fastsat passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser, idet der som anført i forarbejderne er etableret en såkaldt "fast track"-ordning.

Afgørelser efter § 9 a i lov om inddrivelse af gæld til det offentlige antages derfor at kunne foretages i overensstemmelse med forordningens artikel 22, stk. 2, litra b.

Det følger endvidere som et eksempel af § 1, stk. 5, i skattekontrolloven, at skatteministeren fastsætter regler om, at visse selvangivelsespligtige, herunder selvangivelsespligtige, som ifølge lovgivningen forudsættes at indgive en selvangivelse, modtager en årsopgørelse i stedet for en selvangivelse.[484] En årsopgørelse indeholder en opgørelse af borgerens skattepligtige indkomst og beregning af skatten efter reglerne i kildeskattelovens §§ 60-62 og er således en afgørelse. En årsopgørelse vil som udgangspunkt være omfattet af forordningens § 22, stk. 1.

Det fremgår af forarbejderne til § 1, stk. 5[485], at visionen på skatteområdet, herunder for SKATs systemmodernisering af borgerområdet, er, at opgaven med at befatte sig med skat for de allerfleste borgere skal søges reduceret til et minimum, ligesom borgerens behov for kontakt til SKAT skal søges begrænset mest muligt. Endvidere er det sigtet, at kommunikationen mellem skatteyder og SKAT i videst mulige omfang digitaliseres.

Årsopgørelsen dannes automatisk på baggrund af indberetninger fra indberetningspligtige efter skattekontrollovens afsnit II, dvs. pengeinstitutter, pensionsselskaber, fagforeninger, arbejdsgivere m.fl. og eventuelt efter overførsel af oplysninger fra den skattepligtiges egen forskudsopgørelse.

Sådanne automatiske afgørelser vil således have hjemmel i skattekontrollovens § 1, stk. 5, sammenholdt med kildeskattelovens §§ 60-62. Endvidere er der fastsat passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legiti-

[484] Bemyndigelsen efter skattekontrollovs § 1, stk. 5, er udnyttet ved bekendtgørelse nr. 535 af 22. maj 2013, som ændret ved bekendtgørelse nr. 373 af 8. april 2015 om fysiske personers modtagelse af en årsopgørelse i stedet for en selvangivelse.
[485] Forslag til lov nr. L 121 fremsat 11. januar 2006 til lov om ændring af forskellige skattelove. (Enklere forskuds- og selvangivelsesprocedure samt frivillig indberetning af gaver mv.).

me interesser, idet den skattepligtige, hvis denne ikke er enig i årsopgørelsen, kan påklage årsopgørelse til Skatteankestyrelsen efter de almindelige regler i skatteforvaltningsloven. Klagemyndigheden træffer ikke automatisk afgørelse. Afgørelserne vurderes derfor at være i overensstemmelse med forordningens artikel 22, stk. 2, litra b.

Afslutningsvis kan som et yderligere eksempel nævnes, at det følger af kildeskattelovens § 55 B, at SKAT træffer afgørelse om grundlaget for den foreløbige skatteansættelse (forskudsopgørelse). Den ordinære forskudsopgørelse, som udsendes til borgerne i november i året før indkomståret, dannes automatisk på baggrund af oplysninger om den skattepligtiges indkomstforhold, som følger af den seneste årsopgørelse og forskudsopgørelse, løbende oplysninger fra indberetningspligtige efter skattekontrolloven og aktuelle oplysninger fra indkomstregisteret og andre registre, som SKAT modtager oplysninger fra. Forskudsopgørelsen indeholder en opgørelse af den forventede skat, som den skattepligtige skal betale for det kommende indkomstår. Oplysningerne i forskudsopgørelsen ligger til grund for dannelsen af skattekortet til brug for indeholdelse af den skattepligtiges A-skat og indbetalingskort til betaling af B-skat.

I selve indkomståret vil SKAT efter kildeskattelovens § 53, stk. 3, kunne ændre forskudsopgørelsen, hvis den forventede skat afviger fra den beregnede skat ifølge den ordinære forskudsopgørelse, og ændringen overstiger en fast grænse, som er fastsat i kildeskattebekendtgørelsen. Også en sådan ændring dannes automatisk, men den skattepligtige skal efter § 53, stk. 4, have mulighed for inden en frist at fremkomme med sine indvendinger mod ændringen. Har den skattepligtige ikke inden fristens udløb fremkommet med sådanne indvendinger, gennemføres ændringen som varslet uden yderligere underretning af den skattepligtige.

Ovennævnte afgørelser vil have hjemmel i kildeskattelovens § 55 B og § 53, stk. 3, og vil som udgangspunkt være omfattet af forordningens § 22, stk. 1. Endvidere er der fastsat passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser, idet den skattepligtige kan klage til Skatteankestyrelsen over såvel en ordinær som en ændret forskudsopgørelse efter de almindelige regler i skatteforvaltningsloven. Klagemyndigheden træffer ikke automatisk afgørelse. Afgørelserne vurderes derfor at være i overensstemmelse med forordningens artikel 22, stk. 2, litra b.

4.12.3.2.3. Databeskyttelsesforordningens artikel 22, stk. 2, litra c, om samtykke, herunder artikel 22, stk. 3

Det fremgår endelig af databeskyttelsesforordningens artikel 22, stk. 2, *litra c*, at bestemmelsens stk. 1 ikke finder anvendelse, hvis afgørelsen er baseret på den registreredes udtrykkelige samtykke.

Dette samtykke må forstås i overensstemmelse med det samtykke, som følger af forordningens artikel 9, stk. 2, litra a, da det fremgår, at det skal være udtrykkeligt, ligesom samtykket må skulle opfylde betingelserne i forordningens artikel 7.

Der henvises for nærmere om udtrykkeligt samtykke til afsnit 2.3. om definitioner, afsnit 3.5. om betingelser for samtykke, artikel 7 og afsnit 3.8. om hjemler til behandling af følsomme oplysninger, jf. artikel 9, stk. 2-3.

Det fremgår endvidere i forbindelse hermed af forordningens artikel 22, stk. 3, at i de tilfælde, der er omhandlet i stk. 2, litra c, gennemfører den dataansvarlige passende foranstaltninger til at beskytte den registreredes rettigheder og frihedsrettigheder samt legitime interesser, i det mindste den registreredes ret til menneskelig indgriben fra den dataansvarliges side, til at fremkomme med sine synspunkter og til at bestride afgørelsen.

At det fremgår direkte af lovteksten i forordningen, at der kan foretages automatiske individuelle afgørelser, herunder profilering, såfremt afgørelsen er baseret på den registreredes udtrykkelige samtykke er en nyskabelse i forhold til gældende ret. Det fremgår således nu direkte, at der vil kunne indhentes samtykke i den forbindelse.

Artikel 22, stk. 2, litra c, bevirker, at et forsikringsselskab i aftalen med den registrerede eksempelvis vil kunne anmode om den registreredes udtrykkelige samtykke til at foretage automatiske afgørelser.

I den forbindelse bemærkes det, at ved vurderingen af, hvorvidt et samtykke er givet frit efter artikel 7, stk. 4, må der lægges vægt på, at EU-lovgiver har givet mulighed for, at forsikringsselskaber eller andre kan træffe automatiske afgørelser på baggrund af et udtrykkeligt samtykke, jf. artikel 22, stk. 2, litra c.

Et samtykke efter artikel 22, stk. 2, litra c, må således som udgangspunkt anses som værende frivilligt og dermed gyldigt, hvis det i øvrigt lever op til betingelserne for et gyldigt samtykke, herunder i denne sammenhæng særligt kravet om at samtykket skal være informeret.

Der er som tidligere anført det yderligere krav, som følger af artikel 22, stk. 3, hvorefter den dataansvarlige skal gennemføre passende foranstaltninger.

I relation til undtagelsen om samtykke må henvisningen til artikel 22, stk. 3, bevirke, at den dataansvarlige ikke blot vil kunne nøjes med at indhente den registreredes samtykke. Den dataansvarlige vil samtidig have ansvaret for at sikre beskyttelsen af den registreredes

rettigheder og frihedsrettigheder samt legitime interesser, hvorfor samtykke efter artikel 22, stk. 2, litra c, har en yderligere dimension end blot det almindelige samtykke i forordningens forstand.

En passende foranstaltning vil som anført ovenfor eksempelvis kunne være en mulighed for den registrerede til at anmode virksomheden om at genoptage afgørelsen og behandle sagen ved menneskelig indgriben.

I præambelbetragtning nr. 71 er der endelig et fortolkningsbidrag til, hvad den dataansvarlige skal iagttage, når der så foretages automatiske individuelle afgørelser. Det fremgår heraf, at for at sikre en rimelig og gennemsigtig behandling for så vidt angår den registrerede under hensyntagen til de specifikke omstændigheder og forhold, som personoplysningerne behandles under, bør den dataansvarlige anvende passende matematiske eller statistiske procedurer til profileringen, gennemføre tekniske og organisatoriske foranstaltninger, der navnlig kan sikre, at faktorer, der resulterer i unøjagtige personoplysninger, bliver rettet, og at risikoen for fejl minimeres, samt sikre personoplysninger på en måde, der tager højde for de potentielle risici for den registreredes interesser og rettigheder, og som hindrer bl.a. forskelsbehandling af fysiske personer på grund af race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetisk status eller helbredstilstand eller seksuel orientering, eller som resulterer i foranstaltninger, der har en sådan virkning.

Særligt om børn
Det fremgår af præambelbetragtning nr. 71, at behandling efter artikel 22 ikke bør omfatte et barn.

For nærmere om definitionen af "børn" henvises til afsnit 3.6. om betingelser for et barns samtykke i forbindelse med informationssamfundstjenester, artikel 8.

At det nu særligt fremgår af betragtningen, at behandlingen ikke bør omfatte et barn, stemmer godt overens med forordningens røde tråd om, at børn skal nyde en særlig beskyttelse, hvilket eksempelvis kommer til udtryk i artikel 8 om betingelser for et barns samtykke i forbindelse med informationssamfundstjenester.

At det eksplicit fremgår, at automatiske individuelle afgørelser, herunder profilering ikke bør omfatte et barn, er en nyskabelse i forhold til gældende ret. Efter forordningen ses der således at være et udgangspunkt om, at automatiske individuelle afgørelser, herunder profilering overfor et barn, ikke bør finde anvendelse.

Omvendt medfører præambelbetragtning nr. 71 *ikke* et direkte forbud mod behandling af personoplysninger om et barn efter artikel 22, idet præambelbetragtningen ikke er fulgt op af en udtrykkelig bestemmelse herom i artikel 22.

Men præambelbetragtningens ordlyd om, at "behandling ikke bør omfatte barn" er et fortolkningsbidrag til artikel 22 og får derfor særligt indflydelse på eksempelvis vurderingen af, hvornår en afgørelse *betydeligt* påvirker den pågældende.

I relation til myndighedsudøvelse må dette udgangspunkt dog antages kun at gælde, når barnet direkte interagerer med myndigheden, der træffer afgørelsen. Såfremt interaktionen med myndigheden foretages på vegne af barnet af dets forældre eller værge, må det antages, at præambelbetragtning nr. 71 ikke er relevant. Dette må også gælde selvom, at barnet i begge tilfælde er retssubjektet. Dette skyldes, at barnets interesser i disse tilfælde varetages af dets forældre eller værge.

Beskyttelsen fokuseres især på de tilfælde, hvor der sker indsamling af personoplysninger om børn og deres personlige oplysninger i relation til eksempelvis oprettelse af personligheds- eller brugerprofiler, når de anvendte tjenester tilbydes barnet direkte.

Det kan ligeledes fremhæves, at artikel 8 giver indehaveren af forældremyndigheden over barnet muligheden for at samtykke på vegne af barnet.

Særligt om følsomme oplysninger efter artikel 9, stk. 1, jf. databeskyttelsesforordningens artikel 22, stk. 4
Det fremgår af artikel 22, stk. 4, at de afgørelser, der er omhandlet i stk. 2, ikke må baseres på særlige kategorier af personoplysninger, jf. artikel 9, stk. 1, medmindre artikel 9, stk. 2, litra a eller g, finder anvendelse, og der er indført passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser.

Det fremgår yderligere af præambelbetragtning nr. 71, at automatiske afgørelser og profilering baseret på særlige kategorier af personoplysninger kun bør tillades under særlige omstændigheder.

Der vil derfor kun kunne træffes automatiske individuelle afgørelser, herunder profilering vedrørende følsomme oplysninger, når det er baseret på et samtykke efter artikel 9, stk. 2, litra a, eller behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret efter artikel 9, stk. 2, litra g.

Dette samtykke skal opfylde forordningens artikel 4, nr. 11, herunder kravet om frivillighed samt betingelserne i forordningens artikel 7, ligesom samtykket må forstås i overensstemmelse med det samtykke, som følger af forordningens artikel 9, stk. 2, litra a.

For så vidt angår kravet om, at de afgørelser, der er omhandlet i stk. 2, ikke må baseres på særlige kategorier af personoplysninger, jf. artikel 9, stk. 1, medmindre artikel 9, stk. 2, litra g, "finder anvendelse", bevirker dette "blot", at behandlingen skal ligge inden for rammerne af "væsentlige samfundsinteresser".

Derudover er der som anført det yderligere krav i forordningens artikel 22, stk. 4, at der er indført passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser.

Indsættelsen af hensynet til særlige kategorier af personoplysninger, som følger af forordningens artikel 22, stk. 4, er en nyskabelse i forhold til gældende ret. Det er også en nyskabelse, at en eventuel automatisk individuel afgørelse baseret på særlige kategorier af oplysninger, kun vil kunne ske, såfremt artikel 9, stk. 2, litra a, om samtykke eller artikel 9, stk. 2, litra g, om behandling, der er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret, finder anvendelse.

Det er vigtigt at holde sig for øje, at der altså kan indføres nationale regler, som tillader denne behandling under iagttagelse af passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser.

4.12.3.3. Den registreredes rettigheder i forbindelse med automatiske individuelle afgørelser

Efter databeskyttelsesforordningen har den registrerede en række rettigheder i forbindelse med automatiske individuelle afgørelser, herunder profilering efter artikel 22.

Artikel 22 nævnes flere gange i forordningens artikel 12 om gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder.

Heraf følger det blandt andet af artikel 12, stk. 3, at den dataansvarlige uden unødig forsinkelse og i alle tilfælde senest en måned efter modtagelsen af anmodningen oplyser den registrerede om foranstaltninger, der træffes på baggrund af en anmodning i henhold til artikel 22.

Den dataansvarlige har oplysningspligt overfor den registrerede, jf. artikel 13, stk. 2, litra f, og artikel 14, stk. 2, litra g, hvorefter det fremgår, at hvis personoplysninger om en regi-

streret indsamles hos den registrerede, giver den dataansvarlige på det tidspunkt, hvor personoplysningerne indsamles, den registrerede oplysninger om forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og i disse tilfælde som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede.

Endvidere følger det af artikel 15 stk. 1, litra h, at den registrerede har ret til at få den dataansvarliges bekræftelse på, om personoplysninger vedrørende den pågældende behandles, og i givet fald adgang til personoplysningerne og information om forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede.

De rettigheder, som tilkommer den registrerede efter persondatalovens § 39, stk. 3, ses også at blive videreført i databeskyttelsesforordningen.

Det skal dog bemærkes, at der er mulighed for at begrænse den registreredes rettigheder.

Eksempelvis må det antages, at retten til indsigt efter artikel 22 i selve logikken bag en virksomheds afslag på kredit vil kunne begrænses efter eksempelvis forordningens artikel 23, stk. 1, litra i, om beskyttelse af andres rettigheder og frihedsrettigheder af hensyn til virksomhedens forretningshemmeligheder.

For nærmere herom henvises til afsnit 4.13. om begrænsning af rettighederne, artikel 23.

4.12.4. Overvejelser

Databeskyttelsesforordningens artikel 22, stk. 1, er udtryk for en videreførelse af gældende ret, dog med den tilføjelse, at profilering nu direkte nævnes i bestemmelsen, ligesom profilering defineres særskilt i forordningens artikel 4, nr. 4.

Databeskyttelsesforordningens artikel 22, stk. 2, ses endvidere at være en videreførelse af gældende ret – dog er samtykke særskilt fremhævet som begrundelse for, at udgangspunktet om ret til ikke at være genstand for automatiske individuelle afgørelser, herunder profilering, kan fraviges.

I databeskyttelsesforordningen er der derudover en nyskabelse, hvorefter der er et udgangspunkt om, at automatiske individuelle afgørelser, herunder profilering overfor et barn, ikke bør finde anvendelse.

Indsættelsen af hensynet til særlige kategorier af personoplysninger, som følger af forordningens artikel 22, stk. 4, er endvidere en nyskabelse i forhold til gældende ret.

Endelig ses de rettigheder, som tilkommer den registrerede efter persondatalovens § 39, stk. 3, at blive videreført i databeskyttelsesforordningen.

4.13. Begrænsninger af rettighederne, artikel 23

4.13.1. Præsentation

Efter databeskyttelsesdirektivets artikel 13 er der mulighed for, at medlemsstaterne efter en række oplistede hensyn kan træffe lovmæssige foranstaltninger med henblik på at begrænse rækkevidden af udvalgte bestemmelser i databeskyttelsesdirektivet – særligt de registreredes rettigheder og den dataansvarliges pligter af hensyn til den registrerede.

I dansk ret er der på baggrund af direktivet i persondatalovens § 30 fastsat undtagelser til den dataansvarliges oplysningspligt over for den registrerede.

Endvidere er der bl.a. fastsat begrænsninger om den registreredes indsigtsret, jf. persondatalovens § 32, stk. 1, den registreredes indsigelsesret i forbindelse med automatiske individuelle afgørelser, jf. lovens § 39, stk. 3, samt i lovens § 65, som omhandler Datatilsynets årlige beretning.

På tilsvarende vis er der efter databeskyttelsesforordningens artikel 23, stk. 1, mulighed for ved lovgivningsmæssige foranstaltninger i EU-retten eller medlemsstaternes nationale ret at begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 12-22 og 34 samt artikel 5, for så vidt bestemmelserne heri svarer til rettighederne og forpligtelserne i artikel 12-22, når begrænsningerne respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til en række nærmere oplistede hensyn.

Endvidere følger det af databeskyttelsesforordningens artikel 23, stk. 2, at enhver lovgivningsmæssig foranstaltning, som minimum, hvor det er relevant, skal indeholde specifikke bestemmelser vedrørende en række nærmere oplistede forhold.

4.13.2. Gældende ret

Det fremgår af databeskyttelsesdirektivets artikel 13, stk. 1, at medlemsstaterne kan træffe lovmæssige foranstaltninger med henblik på at begrænse rækkevidden af de forpligtelser

og rettigheder, der er omhandlet i artikel 6, stk. 1, artikel 10, artikel 11, stk. 1, samt artikel 12 og 21, hvis en sådan begrænsning er en nødvendig foranstaltning af hensyn til:

> a) statens sikkerhed
> b) forsvaret
> c) den offentlige sikkerhed
> d) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv
> e) væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender
> f) en kontrol-, tilsyns- eller reguleringsopgave, selv af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i litra c, d og e nævnte områder
> g) beskyttelsen af den registreredes interesser eller andres rettigheder og frihedsrettigheder.

Det fremgår endvidere af databeskyttelsesdirektivets artikel 13, stk. 2, at medlemsstaterne med forbehold af de fornødne lovhjemlede garantier, navnlig for, at oplysningerne ikke anvendes til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer, i tilfælde, hvor der klart ikke er nogen risiko for, at den registreredes ret til privatlivets fred krænkes, ved lov kan begrænse de i artikel 12 omhandlede rettigheder, hvis oplysningerne udelukkende behandles med videnskabelig forskning for øje eller kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker.

Det fremgår af præambelbetragtning nr. 42 til databeskyttelsesdirektivet, at medlemsstaterne af hensyn til den registreredes interesser eller med henblik på at beskytte andres rettigheder og frihedsrettigheder kan begrænse retten til indsigt og til underretning. Medlemsstaterne kan f.eks. fastsætte, at adgang til medicinske oplysninger kun kan finde sted via en person, der udøver en profession inden for sundhedsvæsenet.

Det fremgår endvidere af præambelbetragtning nr. 43 til databeskyttelsesdirektivet, at medlemsstaterne ligeledes kan indskrænke retten til indsigt og underretning samt visse af den dataansvarliges forpligtelser, såfremt dette er nødvendigt af hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed eller væsentlige økonomiske og finansielle interesser i medlemsstaten eller Unionen samt efterforskning og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv – undtagelser og begrænsninger bør omfatte kontrol-, tilsyns- og reguleringsopgaver, der er nødvendige på de tre sidstnævnte områder vedrørende den offentlige sikkerhed, de økonomiske og finansielle

interesser og retsforfølgning i straffesager. Dette berører ikke det berettigede i undtagelser og begrænsninger af hensyn til statens sikkerhed eller forsvaret.

Det fremgår i forlængelse heraf endelig af præambelbetragtning nr. 44 til databeskyttelsesdirektivet, at medlemsstaterne i medfør af fællesskabsrettens bestemmelser kan blive nødt til at fravige bestemmelserne i dette direktiv vedrørende indsigt, underretning af de registrerede og oplysningernes kvalitet for at sikre visse af de i betragtning nr. 42 og 43 nævnte mål.

I sag C-473/12, Institut professionel des agents immobiliers (IPI), dom af 7. november 2013, som vedrørte fortolkningen af databeskyttelsesdirektivets artikel 13, stk. 1, anførte EU-Domstolen, at artikel 13, stk. 1, giver medlemsstaterne mulighed for at fastsætte en eller flere af de undtagelser, som artikel 13 opregner, men at medlemsstaterne ikke er tvunget hertil, jf. præmis 37. Dernæst anførte EU-Domstolen, at virksomhed som privatdetektiv, der handler for et fagligt organ for at efterforske brud på etiske regler for et lovreguleret erhverv, er omfattet af den undtagelse, der er fastsat i artikel 13, stk. 1, litra d, om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv, jf. præmis 53.

EU-Domstolen udtalte endelig, at hvis en medlemsstat har valgt at gennemføre den undtagelse, der er fastsat i databeskyttelsesdirektivets artikel 13, stk. 1, litra d, kan det pågældende faglige organ og de privatdetektiver, der handler for dette organ, påberåbe sig denne og er ikke underlagt oplysningspligten over for den registrerede, som fastsat i artikel 10 og 11 i direktivet, jf. præmis 45.

Endvidere kan nævnes sag C-201/14, Bara, dom af 1. oktober 2015, som vedrørte spørgsmålet om, hvorvidt artikel 10, 11 og 13 i databeskyttelsesdirektivet skulle fortolkes således, at bestemmelserne var til hinder for nationale foranstaltninger som tillod en offentlig myndighed i en medlemsstat at videregive personoplysninger til en anden offentlig myndighed og den efterfølgende behandling af oplysningerne, uden at de registrerede på forhånd var blevet underrettet om denne videregivelse og denne behandling. I sagen udtalte EU-Domstolen, at databeskyttelsesdirektivets artikel 13 udtrykkeligt kræver, at begrænsninger af hensyn til »væsentlige økonomiske eller finansielle interesser hos en medlemsstat […], herunder valuta-, budget- og skatteanliggender« samt »en kontrol-, tilsyns- eller reguleringsopgave, selv af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i litra c, d og e nævnte områder« træffes ved lovmæssige foranstaltninger, jf. præmis 39.

I betænkning nr. 1345 anførte Registerudvalget, at den opregning af interesser, som var indeholdt i artikel 13, stk. 1, efter udvalgets opfattelse måtte antages at være udtømmende. Udvalget lagde herved vægt på, at bestemmelsens affattelse talte herfor, samt at det af bestemmelsens tilblivelseshistorie klart fremgik, at der var tale om en udtømmende regulering af, hvilke interesser, der kunne begrunde undtagelser fra de i bestemmelsen nævnte artikler.[486]

Registerudvalget anførte endvidere, at det ikke nærmere fremgik af direktivet, herunder dettes præambel, hvad de nævnte bestemmelser i litra a-g dækkede over. Udvalget fandt dog, at der af bestemmelsens tilblivelseshistorie kunne udledes enkelte fortolkningsbidrag.[487]

Registerudvalget anførte således, at der ved udtrykket "statens sikkerhed", jf. litra a, skulle forstås beskyttelse af den nationale suverænitet mod indre og ydre trusler, som fremgik af Kommissionens bemærkninger til det reviderede direktivforslag (KOM(92) 422 endelig udg. - SYN 287, side 24). Ligesom det ifølge Registerudvalget fremgik af samme sted, at der ved udtrykket "offentlig sikkerhed" skulle forstås alle de politifunktioner, der udføres af statslige organer, herunder kriminalitetsforebyggelse.[488]

Registerudvalget anførte endvidere, at udtrykket "den registreredes interesser eller andres rettigheder og frihedsrettigheder", jf. litra g, dels dækker over den registreredes interesser, dels omfatter en anden persons rettigheder, herunder også den dataansvarliges rettigheder. Disse rettigheder kunne eksempelvis være forretningshemmeligheder, den professionelle tavshedspligt, som læger og advokater skal iagttage, retten til at forberede sit eget forsvar i retssager samt beskyttelse af menneskerettighederne. Udvalget anfører endvidere, at en tilsynsmyndighed f.eks. bør kunne indrømme fritagelser for retten til indsigt for den registrerede med hensyn til oplysninger vedrørende den pågældende selv, der opbevares af menneskerettighedsorganisationer, når en ubegrænset adgang ville kunne bringe andre personer (f.eks. når der er tale om kilder til fortrolige oplysninger) eller disse organisationers vitale interesser i fare.[489]

Registerudvalget fandt - bl.a. i lyset heraf - at den i litra g indeholdte bestemmelse måtte antages at give adgang til at gøre undtagelse af hensyn til andres, herunder den dataansvarliges, væsentlige interesser (rettigheder), samt at væsentlige interesser måtte antages at kunne være af såvel offentlig som privat karakter. Under hensyn hertil fandt udvalget, at

[486] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 302
[487] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 301-303.
[488] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 301-303.
[489] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 301-303.

det ville være foreneligt med bestemmelsen i artikel 13, stk. 1, at det i den fremtidige lovgivning blev foreskrevet, at dataansvarlige – såvel offentlige som private - kan undlade at underrette registrerede personer om indsamling af oplysninger om dem, hvis afgørende hensyn til offentlige interesser, herunder de i litra a-f opregnede interesser, eller til private interesser, herunder til den registrerede selv, taler herimod. Udvalget fandt, at med en sådan ordning sikredes det, at der kunne tages højde for alle de situationer, hvor der forelå en beskyttelsesværdig interesse af henholdsvis offentlig og privat karakter, hvilket eksempelvis ville resultere i, at den dataansvarlige i det konkrete tilfælde kunne undlade at underrette den registrerede om indsamlingen af oplysninger om den pågældende af hensyn til de interesser, som var nævnt i Kommissionens bemærkninger til det reviderede direktivforslag, jf. ovenfor.[490]

Registerudvalget anførte endelig i betænkningen, at muligheden for efter artikel 13, stk. 1, at gøre undtagelse burde udnyttes i forhold til undtagelsesmuligheder til den i artikel 12, litra a, hjemlede indsigtsret, samt med hensyn til artikel 21 om behandlingers offentlige tilgængelighed.[491]

Derimod anførte udvalget, at der efter udvalgets opfattelse ikke burde gøres undtagelse i relation til de i artikel 6 indeholdte principper vedrørende oplysningernes pålidelighed eller med hensyn til reglerne i artikel 12, litra b og c, om den registreredes ret til efter omstændighederne at få oplysninger berigtiget, slettet eller blokeret og i den forbindelse få givet tredjemand underretning herom.[492] Der blev således ikke fastsat begrænsninger herom i persondataloven.

Efter gældende ret er det således inden for det nationale råderum, som databeskyttelsesdirektivet fastlægger, muligt at vedtage særlovgivning.

I dansk ret er det i persondatalovens § 30 fastsat, at bestemmelserne i § 28, stk. 1, og § 29, stk. 1, om oplysningspligt ikke gælder, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til *private* interesser, herunder hensynet til den pågældende selv.

Det følger endvidere af persondatalovens § 30, stk. 2, at undtagelse fra bestemmelserne i § 28, stk. 1, og § 29, stk. 1, tillige kan gøres, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til *offentlige* interesser, herunder navnlig til:

[490] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 301-303.
[491] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 301-302.
[492] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 301-302.

1) statens sikkerhed,
2) forsvaret,
3) den offentlige sikkerhed,
4) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv,
5) væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender, og
6) kontrol-, tilsyns- eller reguleringsopgaver, herunder opgaver af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i nr. 3-5 nævnte områder.

Denne bestemmelse er baseret på databeskyttelsesdirektivets artikel 13, stk. 1, hvorefter medlemsstaterne som anført gives mulighed for at begrænse rækkevidden af nogle af forpligtelserne og rettighederne i databeskyttelsesdirektivet.

Registerudvalget anførte vedrørende persondatalovens § 30, at med en sådan ordning sikredes det, at der kunne tages højde for alle de situationer, hvor der forelå en beskyttelsesværdig interesse af henholdsvis offentlig og privat karakter. Eksempelvis ville den dataansvarlige i det konkrete tilfælde kunne undlade at underrette den registrerede om indsamlingen af oplysninger om den pågældende af hensyn til de interesser, som var nævnt i databeskyttelsesdirektivet.[493]

Efter persondataloven finder begrænsningerne i lovens § 30 bl.a. også anvendelse på den registreredes indsigtsret, jf. persondatalovens § 32, stk. 1, den registreredes indsigelsesret i forbindelse med automatiske individuelle afgørelser, jf. lovens § 39, stk. 3 samt på lovens § 65, som omhandler Datatilsynets årlige beretning.

Som tidligere anført fremgår det af betænkning nr. 1345, at bestemmelsen i persondatalovens § 30, stk. 1, om begrænsning af oplysningspligten af hensyn til afgørende hensyn til private interesser, er fastsat på baggrund af muligheden herfor i databeskyttelsesdirektivets artikel 13, stk. 1, litra g, om beskyttelse af den registreredes interesser eller andres rettigheder og frihedsrettigheder.

Det fremgår af bemærkningerne til persondataloven, at indskrænkningen i den dataansvarliges eller dennes repræsentants oplysningspligt kun kan ske på baggrund af en konkret afvejning af de modstående interesser, som er nævnt i bestemmelsen. Afvejningen må fore-

[493] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 303.

tages for hver enkelt oplysning for sig med den virkning, at der, såfremt sådanne hensyn kun gør sig gældende for en del af de i § 28, stk. 1, og § 29, stk. 1, nævnte oplysninger, skal gives den registrerede meddelelse om de øvrige oplysninger.[494]

Det fremgår endvidere af bemærkningerne, at der i afvejningen på den ene side indgår den registreredes interesse i at få kendskab til de i § 28, stk. 1, og § 29, stk. 1, nævnte oplysninger. Heroverfor står hensynet til private interesser, herunder til den pågældende selv. De private interesser, som kan beskyttes efter bestemmelsen, er såvel den dataansvarliges som tredjemands interesser. Som private interesser, der bl.a. vil kunne begrunde hemmeligholdelse, kan nævnes forretningshemmeligheder, den professionelle tavshedspligt, som læger og advokater skal iagttage, retten til at forberede sit eget forsvar i retssager samt beskyttelse af menneskerettighederne.[495]

Det fremgår yderligere af bemærkningerne, at med anvendelsen af udtrykket »afgørende« er det tilkendegivet, at undtagelse fra oplysningspligten kun kan gøres, hvor der er nærliggende fare for, at privates interesser vil lide skade af væsentlig betydning.[496]

Vedrørende persondatalovens § 30, stk. 2, om begrænsning af oplysningspligten af afgørende hensyn til offentlige interesser, fremgår det endelig af bemærkningerne, at bestemmelsen – ligesom bestemmelsen i stk. 1 – fastsætter, at indskrænkning i den dataansvarliges eller dennes repræsentants oplysningspligt kun kan ske på grundlag af en konkret afvejning af de modstående interesser, som er nævnt i bestemmelsen. På baggrund af en sådan afvejning vil undtagelse kunne gøres, hvis der er nærliggende fare for, at det offentliges interesser vil lide skade af væsentlig betydning.[497]

I en sag vedrørende oplysningspligt i forhold til børn og unge udtalte Datatilsynet, at tilsynet tidligere havde tilkendegivet, at der skulle udøves forsigtighed ved anvendelsen af undtagelsesbestemmelsen i persondatalovens § 30. Datatilsynet udtalte endvidere, at tilsynet imidlertid fandt det nærliggende, at der i visse sociale og familieretlige sager kunne foreligge sådanne afgørende hensyn, at de kunne begrunde en fravigelse af oplysningspligten over for børn og unge.[498]

---

[494] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 30.
[495] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 30.
[496] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 30.
[497] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 30.
[498] Sag vedrørende oplysningspligt i forhold til børn og unge, Datatilsynets j.nr. 2003-321-0243.

Databeskyttelsesdirektivets artikel 13, stk. 1, giver som anført mulighed for at begrænse rækkevidden af nogle af forpligtelserne og rettighederne i databeskyttelsesdirektivet.

Visse tavshedspligtsbestemmelser i særlovgivningen udnytter denne mulighed, eksempelvis arbejdsmiljølovens § 79, stk. 2, som fastslår, at Arbejdstilsynet ikke over for arbejdsgiveren eller andre må oplyse, at Arbejdstilsynet har modtaget en klage over arbejdsmiljøet hos arbejdsgiveren. En tilsvarende bestemmelse findes på socialtilsynsområdet i § 11, stk. 3, i bekendtgørelse nr. 70 af 18. januar 2017 af lov om socialtilsyn

Der er endvidere for Finanstilsynets ansatte en særlig tavshedspligt i medfør af § 354, stk. 1, i lov om finansiel virksomhed. Det følger heraf, at Finanstilsynets ansatte er forpligtet til efter straffelovens §§ 152-152 e, at hemmeligholde fortrolige oplysninger, som de får kendskab til gennem tilsynsvirksomheden. Med fortrolige oplysninger menes der oplysninger om en finansiel virksomheds forretningsmæssige forhold og kunders forhold samt andre oplysninger, som efter deres karakter er fortrolige.

4.13.3. Databeskyttelsesforordningen

4.13.3.1. Databeskyttelsesforordningens artikel 23, stk. 1 – mulighed for at begrænse ved at fastsætte lovmæssige foranstaltninger i national ret

Det fremgår af artikel 23, stk. 1, i databeskyttelsesforordningen, at EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige eller databehandleren er underlagt, ved lovgivningsmæssige foranstaltninger kan begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 12-22 og 34 samt artikel 5, for så vidt bestemmelserne heri svarer til rettighederne og forpligtelserne i artikel 12-22, når en sådan begrænsning respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til:

a) statens sikkerhed
b) forsvaret
c) den offentlige sikkerhed
d) forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed
e) andre vigtige målsætninger i forbindelse med beskyttelse af Unionens eller en medlemsstats generelle samfundsinteresser, navnlig Unionens eller en medlemsstats væsentlige økonomiske eller finansielle interesser, herunder valuta-, budget- og skatteanliggender, folkesundhed og social sikkerhed
f) beskyttelse af retsvæsenets uafhængighed og retssager

g) forebyggelse, efterforskning, afsløring og retsforfølgning i forbindelse med brud på etiske regler for lovregulerede erhverv
h) kontrol-, tilsyns- eller reguleringsfunktioner, herunder opgaver af midlertidig karakter, der er forbundet med offentlig myndighedsudøvelse i de tilfælde, der er omhandlet i litra a)-e) og g)
i) beskyttelse af den registrerede eller andres rettigheder og frihedsrettigheder
j) håndhævelse af civilretlige krav.

Det fremgår af præambelbetragtning nr. 73, at specifikke principper og retten til oplysninger, indsigt i og berigtigelse eller sletning af personoplysninger, retten til dataportabilitet, retten til indsigelse, afgørelser baseret på profilering og meddelelse af et brud på persondatasikkerheden til en registreret og visse tilknyttede forpligtelser for de dataansvarlige kan begrænses af EU-retten eller medlemsstaternes nationale ret, for så vidt det er nødvendigt og forholdsmæssigt i et demokratisk samfund af hensyn til den offentlige sikkerhed, herunder beskyttelse af menneskeliv, især som reaktion på naturkatastrofer eller menneskeskabte katastrofer, forebyggelse, efterforskning og retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed, eller brud på de etiske regler for lovregulerede erhverv, andre af Unionens eller en medlemsstats samfundsinteresser, navnlig Unionens eller en medlemsstats vigtige økonomiske eller finansielle interesser, føring af offentlige registre i offentlighedens interesse, viderebehandling af arkiverede personoplysninger for at tilvejebringe specifikke oplysninger om politisk adfærd under tidligere totalitære regimer eller beskyttelse af den registrerede eller andres rettigheder og frihedsrettigheder, herunder social sikring, folkesundhed og humanitære formål.

Det fremgår endvidere af præambelbetragtning nr. 73, at en sådan begrænsning bør være i overensstemmelse med kravene i chartret og i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder.

Efter databeskyttelsesforordningens artikel 23, stk. 1, ses der på baggrund af en ordlydsfortolkning at være samme mulighed for at lave begrænsninger i forskellige bestemmelser i forordningen ved EU-ret eller medlemsstaternes nationale ret, som der var efter databeskyttelsesdirektivet, jf. dog om forordningens artikel 23, stk. 2, nedenfor.

Databeskyttelsesforordningen indeholder endda yderligere mulighed – end hvad der fulgte af databeskyttelsesdirektivet – for også at begrænse bestemmelserne i henholdsvis artikel 20 om ret til dataportabilitet, artikel 21 om indsigelse, artikel 22 om automatiske individu-

elle afgørelser, herunder profilering samt artikel 34 om underretning om brud på persondatasikkerheden til den registrerede.

Forordningens artikel 23, stk. 1, litra a-j, indeholder som anført en række hensyn, hvorefter der i en national lov kan fastsættes begrænsninger af udvalgte bestemmelser i forordningen. Disse hensyn ses at svare til de hensyn, som er oplistet i databeskyttelsesdirektivets artikel 13, stk. 1, litra a-g. Dog indeholder forordningen en række yderligere hensyn, som ikke var direkte iagttaget i databeskyttelsesdirektivet, eksempelvis hensynet til "forebyggelse af trusler mod den offentlige sikkerhed", jf. artikel 23, stk. 1, litra d, "håndhævelse af civilretlige krav", jf. artikel 23, stk. 1, litra j, mv.

Det bemærkes, at det fremgår af persondatalovens § 30, stk. 1, at bestemmelserne i § 28, stk. 1, og § 29, stk. 1, om oplysningspligt ikke gælder, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til *private* interesser. En sådan undtagelsesmulighed må fremover kunne ligge inden for rammerne af forordningens artikel 23, stk. 1, litra i, om beskyttelsen af *andres rettigheder og frihedsrettigheder*.

Databeskyttelsesforordningens artikel 23, stk. 1, ses således at indeholde tilsvarende *mulighed* for at fastsætte begrænsninger i forordningens bestemmelser, som det var tilfældet efter databeskyttelsesdirektivets artikel 13. Det står medlemsstaterne frit for at udnytte undtagelsesmuligheden, herunder alene at udnytte denne i begrænset omfang. Dog vil forordningens artikel 23, stk. 1, indeholde rum til at fastsætte begrænsninger i flere bestemmelser i forordningen, ligesom forordningens artikel 23, stk. 1, oplister flere hensyn i bestemmelsens litra a-j, hvorefter der kan fastsættes begrænsninger, end det var tilfældet efter direktivet.

Databeskyttelsesdirektivets artikel 13, stk. 2, indeholder som nævnt mulighed for, at ved lov at begrænse de i artikel 12 omhandlede rettigheder, hvis oplysningerne udelukkende behandles med videnskabelig forskning for øje eller kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker, med forbehold af de fornødne lovhjemlede garantier, navnlig for at oplysningerne ikke anvendes til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer, i tilfælde, hvor der klart ikke er nogen risiko for, at den registreredes ret til privatlivets fred krænkes. Denne bestemmelse bliver ikke direkte videreført i databeskyttelsesforordningen, men derimod er der bestemmelser om begrænsning af hensyn til videnskabelige eller historiske forskningsformål eller til statistiske formål samt arkivformål i samfundets interesse i databeskyttelsesforordningens artikel 89, stk. 2-3.

For nærmere herom henvises til afsnit 10.5. om en nærmere analyse af rammerne i artikel 89, stk. 1 og 2 samt 4, vedrørende videnskabelige og historiske forskningsformål og statistiske formål og afsnit 10.6. om en nærmere analyse af rammerne i artikel 89, stk. 1 og 3 samt 4, vedrørende arkivformål i samfundets interesse.

4.13.3.2. Databeskyttelsesforordningens artikel 23, stk. 2 – krav om specifikke bestemmelser, som minimum, hvor det er relevant

Det fremgår endvidere af databeskyttelsesforordningens artikel 23, stk. 2, at navnlig skal enhver lovgivningsmæssig foranstaltning, der er omhandlet i stk. 1, *som minimum, hvor det er relevant*, indeholde *specifikke* bestemmelser vedrørende:

a) formålene med behandlingen eller kategorierne af behandling
b) kategorierne af personoplysninger
c) rækkevidden af de indførte begrænsninger
d) garantierne for at undgå misbrug eller ulovlig adgang eller overførsel
e) specifikation af den dataansvarlige eller kategorierne af dataansvarlige
f) opbevaringsperioder og de gældende garantier under hensyntagen til behandlingens karakter, omfang og formål eller kategorier af behandling
g) risiciene for de registreredes rettigheder og frihedsrettigheder, og
h) de registreredes ret til at blive underrettet om begrænsningen, medmindre dette kan skade formålet med begrænsningen.

Databeskyttelsesforordningens artikel 23, stk. 2, indeholder krav til de lovmæssige foranstaltninger, som fastsættes efter bestemmelsens stk. 1.

Hensynene i bestemmelsen er en nyskabelse i forhold til databeskyttelsesdirektivet, og det er derfor et nyt krav, at de lovmæssige foranstaltninger, hvor det er relevant, skal indeholde specifikke bestemmelser vedrørende en række oplistede hensyn, jf. artikel 23, stk. 2, litra a-h.

På baggrund af denne bestemmelse ses det at have været vigtigt for EU-lovgiver at fremhæve, at begrænsninger af bl.a. de registreredes rettigheder, skal iagttage en række hensyn, som i videre omfang end hidtil forsøger at tilgodese de personer, som begrænsningen efter stk. 1, vedrører.

Forordningens artikel 23, stk. 2, indeholder ikke noget absolut krav om, at der i bestemmelser, hvorefter eksempelvis den registreredes rettigheder begrænses efter artikel 23, stk. 1, *skal* være specifikke bestemmelser vedrørende den oplistede række hensyn. Dette fremgår klart af bestemmelsen, idet det fremhæves, at lovgivningsmæssige foranstaltninger efter stk. 1, *som minimum, hvor det er relevant,* skal indeholde specifikke bestemmelser

vedrørende en række nærmere oplistede hensyn i litra a-h. Vurderingen af, hvornår det er "relevant" at fastsætte specifikke bestemmelser efter artikel 23, stk. 2, foretages nationalt af lovgiver i forbindelse med udarbejdelsen af loven.

Der er ikke noget fortolkningsbidrag til bestemmelsens ordlyd om "som minimum, hvor det er relevant", hvorfor forordningens artikel 23, stk. 2, forventeligt vil blive udviklet gennem praksis i de kommende år.

4.13.3.3. Nationalt råderum

Ordlyden i databeskyttelsesforordningens artikel 23, stk. 1, bevirker, at der ses at være samme nationale råderum for at begrænse rækkevidden af en række bestemmelser, særligt om den registreredes rettigheder, ved lovgivningsmæssige foranstaltninger, som efter databeskyttelsesdirektivet, idet forordningen endda har lidt flere tilføjelser til, hvornår bestemmelser kan begrænses.

Det er medlemsstaterne og EU-lovgiver, som overlades muligheden for at fastsætte lovgivningsmæssige begrænsninger.

Retstilstanden for det nationale råderum efter artikel 23, stk. 1, ses at være en videreførelse af den gældende retstilstand efter databeskyttelsesdirektivet.

Der ses ikke at være noget krav til de lovgivningsmæssige foranstaltninger efter artikel 23, stk. 1 – udover hvad der følger af artikel 23, stk. 2. Kodeordet i forbindelse med databeskyttelsesforordningens artikel 23 er, at lovgiver ved *"lovgivningsmæssige foranstaltninger"* kan begrænse rækkevidden af en række bestemmelser, når en sådan begrænsning respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til oplistningen i litra a-j.

Det bemærkes således, at der efter forordningens artikel 23, stk. 1, ikke ses at være nogen begrænsning om, at disse lovgivningsmæssige foranstaltninger skal vedrøre særlige specifikke bestemmelser, som det er tilfældet efter eksempelvis artikel 6, stk. 2-3. Der ses således ikke at være noget krav om, at bestemmelsen enten skal være vertikalt eller horisontalt begrænset.

Dette ses også ved, at man i dansk ret på baggrund af databeskyttelsesdirektivets artikel 13, stk. 1, litra g – som forordningens artikel 23, stk. 1, litra i, svarer til – i persondatalovens § 30 fastsatte en generel begrænsning af persondatalovens regler (baseret på direktivet) om oplysningspligt.

Efter artikel 23, stk. 1, ses der således ikke at være noget til hinder for i en *generel lov* at opretholde eller indføre lovgivningsmæssige foranstaltninger om begrænsninger, der eksempelvis svarer til persondatalovens §§ 30 og 32, stk. 1. Derudover skal lovgiver iagttage forordningens artikel 23, stk. 2.

Det bemærkes, at der efter artikel 23 er strenge krav til, hvornår rækkevidden af forpligtelser og rettigheder kan begrænses, idet de lovgivningsmæssige foranstaltninger skal respektere det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder, og begrænsningen skal være en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund efter den oplistning af hensyn, som fremgår af forordningens artikel 23, stk. 1, litra a-j.

Som tidligere anført indeholder artikel 23, stk. 2, ikke et absolut krav, særligt som følge af vendingen "hvor relevant".

Det fremgår i den forbindelse som et fortolkningsbidrag til udtrykket "lovgivningsmæssig foranstaltning" i artikel 23, stk. 2, af præambelbetragtning nr. 41, at når forordningen henviser til et retsgrundlag eller en lovgivningsmæssig foranstaltning, kræver det ikke nødvendigvis en lov, der er vedtaget af et parlament, med forbehold for krav i henhold til den forfatningsmæssige orden i den pågældende medlemsstat. Et sådant retsgrundlag eller en sådan lovgivningsmæssig foranstaltning bør imidlertid være klar(t) og præcis(t), og anvendelse heraf bør være forudsigelig for personer, der er omfattet af dets/dens anvendelsesområde, jf. retspraksis fra EU-Domstolen og Den Europæiske Menneskerettighedsdomstol.

Præambelbetragtning nr. 41 sammenholdt med, at artikel 23, stk. 2, ikke indeholder et absolut krav, bevirker, at der i en dansk sammenhæng ikke vil være noget til hinder for, at hensynene i artikel 23, stk. 2, ikke fremgår direkte af lovteksten til en generel lov.

Ved en generel lov vil det således ikke nødvendigvis være "relevant" at regulere direkte i lovteksten, hvilke hensyn den dataansvarlige skal tage – da disse hensyn vil kunne variere meget. Det vil til gengæld være relevant nærmere at beskrive de hensyn, jf. artikel 23, stk. 2, litra a-h, som den dataansvarlige skal tilgodese i forarbejderne til den generelle lov. Dette støttes også af præambelbetragtning nr. 41.

Det må på den baggrund antages, at bestemmelsen i persondatalovens § 30 vil kunne opretholdes i en ny udgave af persondataloven, idet den er baseret på databeskyttelsesdirektivets artikel 13, stk. 1, som forordningens artikel 23, stk. 1, er en videreførelse af. Samtidig kan forordningens artikel 23, stk. 2, håndteres ved, at der i forarbejderne til en ny version af persondatalovens § 30, lægges "bånd" på den dataansvarlige. Det kan således i forarbej-

derne pålægges den dataansvarlige at varetage de relevante hensyn i forordningens artikel 23, stk. 2, litra a-h.

En sådan begrænsning af den dataansvarlige kan eksempelvis være, at den dataansvarlige skal foretages en *konkret vurdering*, hvor der skal tages hensyn til legitime interesser – hvilket stemmer overens med Registerudvalgets overvejelser i forbindelse med indførelsen af persondatalovens § 30, som tidligere nævnt.

Endvidere vil der også efter artikel 23, stk. 1, være mulighed for i en *specifik lov* at opretholde eller indføre lovmæssige foranstaltninger om begrænsninger. Dog skal lovgiver også her være opmærksom på forordningens artikel 23, stk. 2.

I en specifik lov – som eksempelvis helt afskærer indsigtsretten for en bestemt sagstype – vil det være mere nærliggende end i en generel lov, at der i selve lovteksten fastsættes specifikke bestemmelser vedrørende de hensyn, som følger af artikel 23, stk. 2, litra a-h.

Eksempelvis vil det være relevant, hvis man i konkurrencesager vælger helt at afskære muligheden for indsigtsret, at det fremgår af selve lovteksten, at indsigtsretten kun er begrænset i situationer, hvor Konkurrence- og Forbrugerstyrelsen er dataansvarlig (artikel 23, stk. 2, litra e), og at formålet med behandlingen er at føre det fornødne tilsyn med, at reglerne i konkurrenceloven ikke overtrædes (artikel 23, stk. 2, litra a). Hvis man i konkurrencesager også vælger at begrænse underretningspligten, vil det ligeledes kunne være relevant, at formålene med behandlingen eller kategorierne af behandlinger fremgår af selve lovteksten (artikel 23, stk. 2, litra a).

Der er dog heller ikke ved en specifik lov et krav om, at hensynene i artikel 23, stk. 2, litra a-h, *skal* fremgå af lovteksten. Eksempelvis vil det være relevant at håndtere artikel 23, stk. 2, litra d, om garantier for at undgå misbrug, at man i forarbejderne adresserer, hvordan man vil undgå misbrug.

For den eksisterende særlovgivning vil dette betyde, at medlemsstaterne som udgangspunkt kan *opretholde* nationale bestemmelser, som begrænser de registreredes rettigheder mv., jf. forordningens artikel 23, stk. 1.

Således vil eksisterende lovgivning, som i forbindelse med udarbejdelsen af lovforslaget eller den pågældende bekendtgørelse blev vurderet som værende i overensstemmelse med databeskyttelsesdirektivets artikel 13 om undtagelser og begrænsninger, antages at kunne bestå.

Der vil dog være det yderligere krav, at de nationale bestemmelser også skal iagttage forordningens artikel 23, stk. 2, hvorfor det vil være nødvendigt at overveje, om de hensyn, som fremgår af artikel 23, stk. 2, litra a-h, blev tilstrækkeligt iagttaget, *som minimum, hvor det var relevant,* i forbindelse med udarbejdelsen af loven eller bekendtgørelsen.

Eksempelvis må det antages, at sundhedslovens § 37, stk. 3, hvoraf det følger, at for optegnelser journalført før den 1. januar 2010 kan retten til aktindsigt efter sundhedslovens § 37, stk. 1, begrænses, i det omfang patientens interesse i at blive gjort bekendt med oplysningerne findes at burde vige for afgørende hensyn til den pågældende selv eller til andre private interesser, vil kunne opretholdes, når forordningen finder anvendelse den 25. maj 2018.

Sundhedslovens § 37, stk. 3, antages at kunne opretholdes, når forordningen finder anvendelse, idet lovgiver i forarbejderne har iagttaget bl.a. databeskyttelsesdirektivets artikel 13, litra g – som svarer til databeskyttelsesforordningens artikel 23, stk. 1, litra i – ved at anføre, at der vil være mulighed for at begrænse patientens ret til aktindsigt, hvis dette er nødvendigt til beskyttelse af den pågældendes interesser eller andres rettigheder. Lovgiver har i øvrigt i forarbejderne iagttaget hensynene bag forordningens artikel 23, stk. 2, litra c, om specifikke bestemmelser vedrørende rækkevidden af de indførte begrænsninger ved at anføre, at undtagelsesbestemmelsen kun har været brugt yderst lidt, og artikel 23, stk. 2, litra g, om specifikke bestemmelser vedrørende risiciene for de registreredes rettigheder og frihedsrettigheder.

4.13.4. Overvejelser

Databeskyttelsesforordningens artikel 23, stk. 1, indeholder samme mulighed for at fastsætte begrænsninger i forordningens bestemmelser, som det var tilfældet efter databeskyttelsesdirektivets artikel 13. Dog vil forordningens artikel 23, stk. 1, indeholde rum til at fastsætte begrænsninger i flere bestemmelser, ligesom forordningens artikel 23, stk. 1, oplister flere hensyn, hvorefter der kan fastsættes begrænsninger, efter bestemmelsens litra a-j, end det var tilfældet efter databeskyttelsesdirektivet.

Artikel 23, stk. 2, er en nyskabelse i forhold til gældende ret.

Medlemsstaternes mulighed for at opretholde og indføre lovgivningsmæssige foranstaltninger i overensstemmelse med forordningens artikel 23, stk. 1, vil ikke være ændret i forhold til gældende ret. Dog indeholder artikel 23, stk. 2, yderligere nye krav til de lovgivningsmæssige foranstaltninger fastsat på baggrund af artikel 23, stk. 1.

Det bemærkes, at hvis bestemmelsen i persondatalovens § 30 opretholdes i en ny udgave af persondataloven, bør der i den forbindelse sikres kongruens mellem persondatalovens § 30 og offentlighedslovens § 8 om egenacces samt forvaltningslovens §§ 15, 15 a og 15 b om undtagelse af oplysninger, hvis ordlyd er henholdsvis "afgørende vægt" og "afgørende hensyn".

5. Forordningens kapitel IV: Dataansvarlig og databehandler

5.1. Den dataansvarliges ansvar, artikel 24

5.1.1 Præsentation

Formålet med en nærmere angivelse af den dataansvarliges ansvar i databeskyttelseslovgivningen er at skabe klarhed over, at det er den dataansvarlige, der som udgangspunkt er ansvarlig for overholdelsen af databeskyttelsesretten. Identificeringen af ansvaret for behandlingen betyder ligeledes, at der skabes klarhed over hvem, de registrerede kan udøve deres rettigheder efter databeskyttelsesretten over for, herunder bl.a. retten til at blive glemt, retten til indsigt samt retten til oplysning mv.

5.1.2. Gældende ret

Der er ikke i gældende ret en eksplicit og overordnet bestemmelse om den dataansvarliges ansvar. I stedet følger dette implicit af henholdsvis definitionen af "den dataansvarlige" samt de krav og forpligtelser, som den dataansvarlige er underlagt i de øvrige bestemmelser af gældende ret.

Det følger således af definitionen af "den dataansvarlige" i persondatalovens § 3, nr. 4, at det er denne, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger. Det følger hermed af bestemmelsens ordlyd, at det er den dataansvarlige, som har retten til at disponere og bestemme over de pågældende personoplysninger, og dermed har den faktiske indflydelse på behandlingen af oplysningerne. Det er derfor som udgangspunkt også den dataansvarlige, der er ansvarlig for overholdelse af databeskyttelsesretten ved behandling af personoplysninger.

Den dataansvarliges ansvar fastlægges nærmere i artikel 6, stk. 2, i databeskyttelsesdirektivet, som persondataloven implementerer i dansk ret. Det følger heraf, at det påhviler den dataansvarlige at sikre, at bestemmelserne i artikel 6, stk. 1, om de grundlæggende behandlingsprincipper for behandling af personoplysninger overholdes.[499] For så vidt angår ordlyden af artikel 6, stk. 2, er denne ikke direkte affattet i persondatalovens § 5. Det må imidlertid lægges til grund, at det implicit følger af bestemmelsen, at det påhviler den dataansvarlige at sikre, at de grundlæggende principper i lovens § 5 ved behandling af personoplysninger overholdes.

Den dataansvarlige er endvidere efter persondatalovens afsnit III om de registreredes rettigheder den, som de registrerede kan udøve deres rettigheder efter persondataloven over-

[499] Artikel 29-gruppens udtalelse nr. 173/2010 om princippet om ansvarlighed (WP), s. 4.

for. Dermed består den dataansvarliges ansvar desuden i at sikre overholdelsen af de registreredes rettigheder efter persondataloven.

Herudover følger det af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Det kan på baggrund af bestemmelsens ordlyd lægges til grund, at den dataansvarlige har ansvaret for, at disse fornødne sikkerhedsmæssige krav gennemføres ved behandling af personoplysninger.

For så vidt angår de typer af foranstaltninger, som den dataansvarlige har ansvaret for at gennemføre, henvises der til afsnit 5.10. om databeskyttelsesforordningens artikel 32 om behandlingssikkerhed.

I henhold til de nuværende regler i persondataloven består den dataansvarliges ansvar således i at overholde de i persondatalovens fastsatte principper og forpligtelser.

5.1.3. Databeskyttelsesforordningen

I databeskyttelsesforordningens artikel 4, nr. 7, defineres en dataansvarlig, som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret.

Denne bestemmelse svarer til artikel 2, litra d, i databeskyttelsesdirektivet.

Som en nyskabelse er der i databeskyttelsesforordningens artikel 24 en eksplicit angivelse af den dataansvarliges ansvar efter forordningen. Det følger således af forordningens artikel 24, stk. 1, om den dataansvarliges ansvar, at denne under hensyntagen til behandlingens karakter, sammenhæng, omfang og formål samt sandsynligheden for og graden af de risici, der er for den registreredes rettigheder og frihedsrettigheder, skal gennemføre passende tekniske og organisatoriske foranstaltninger og kunne demonstrere, at behandlingen af personoplysninger er i overensstemmelse med forordningen. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

Denne overordnede bestemmelse om den dataansvarliges ansvar understreger det nødvendige i, at den dataansvarlige, ud over kravene i de øvrige bestemmelser i forordningen, gennemfører passende tekniske og organisatoriske foranstaltninger, som svarer til de risici, som den pågældende behandling kan medføre for de registrerede. Ligeledes skal den dataansvarlige efter bestemmelsen sikre de pågældende foranstaltningers effektivitet og samtidig kunne påvise, at disse foranstaltninger er truffet.

Tankegangen om ansvarlighed i artikel 24 udmøntes også i andre bestemmelser i forordningen, såsom artikel 30 om fortegnelser over behandlingsaktiviteter og artikel 35 om konsekvensanalyse vedrørende databeskyttelse.

For så vidt angår sammenhængen mellem den dataansvarliges ansvar i artikel 24 og kravene til behandlingssikkerhed i artikel 32, er der tale om to forskellige krav, der som udgangspunkt begge skal efterleves ved behandling af personoplysninger. Det særlige ved artikel 24 er dog, at det alene er den dataansvarlige, som er underlagt denne forpligtelse, hvor det i artikel 32 både er den dataansvarlige og databehandleren, som er forpligtede.

Det præciseres ikke nærmere i artikel 24, stk. 1, hvilke typer af foranstaltninger der kan anses for passende. Dette beror således på en konkret vurdering, som skal foretages af den dataansvarlige. Databeskyttelsesreglerne er horisontale og berører mange livsområder, hvorfor kravene til dataansvarlige vil variere.

De kriterier, der skal anvendes til at vurdere, hvilken type foranstaltninger der bør træffes, er behandlingens karakter, sammenhæng, omfang og formål samt de risici for de registreredes rettigheder og frihedsrettigheder, som databehandlingen indebærer. For så vidt angår vurderingen af risici, betyder dette, at graden af risikoen for den registreredes grundlæggende rettigheder og frihedsrettigheder er bestemmende for, hvilke foranstaltninger der er passende til den pågældende behandling.

Artikel 29-gruppen har i en udtalelse om princippet om ansvarlighed bl.a. anført, at omfanget af databehandling og antallet af planlagte dataoverførsler, bør være afgørende for vurderingen af en behandlingsaktivitets risikoniveau.[500]

Endvidere anbefaler Artikel 29-gruppen, at store dataansvarlige bør gennemføre strenge foranstaltninger, og at mindre eller mellemstore dataansvarlige i tilfælde af, at de er involveret i risikobetonede behandlinger af personoplysninger, f.eks. databehandling på e-sundhedsområdet, ligeledes bør træffe skrappe forholdsregler.

[500] Artikel 29-gruppens udtalelse nr. 173/2010 om princippet om ansvarlighed (WP), s. 14.

Af konkrete typer af foranstaltninger, der som udgangspunkt kan sikre efterlevelse af databeskyttelsesreglerne, nævner Artikel 29-gruppen bl.a. kortlægning af procedurer hos den dataansvarlige for at sikre, at alle databehandlinger kan identificeres, og der kan føres fortegnelse over disse.[501]

Desuden nævner Artikel 29-gruppen uddannelse af personale hos den dataansvarlige i databeskyttelse, etablering af interne procedurer for henholdsvis sikkerhedsbrister, anmodninger fra de registrerede om indsigt, korrektion eller sletning samt udarbejdelse af mekanismer til behandling af klager mv., som passende tekniske og organisatoriske foranstaltninger.

Hvis det er proportionalt i forhold til den behandling af personoplysninger, som finder sted, skal de foranstaltninger, som iværksættes efter artikel 24, stk. 1, omfatte den dataansvarliges implementering af passende databeskyttelsespolitikker, jf. artikel 24, stk. 2.

Disse politikker kan f.eks. bestå af interne politikker og procedurer til behandling af anmodninger om indsigt, klager fra de registrerede mv. De pågældende politikker må ligeledes antages at skulle være relevante og tilstrækkelige i forhold til, hvad der kræves til at opfylde formålet med at efterleve forordningens krav om den dataansvarliges ansvar efter artikel 24, stk. 1.

Disse databeskyttelsespolitikker skal alene gennemføres efter § 24, stk. 2, hvis det er proportionalt i forhold til de behandlingsaktiviteter, som den dataansvarlige udfører. Hertil kræves, at disse skal stå i et rimeligt forhold til de behandlingsaktiviteter, som den dataansvarlige foretager.

Såfremt den dataansvarlige f.eks. alene foretager behandling, som ikke kræver identifikation af den registrerede omfattet af forordningens artikel 11, vil det formentlig ikke være proportionalt for den dataansvarlige at skulle indføre databeskyttelsespolitikker vedrørende interne procedurer for retten til at blive glemt efter artikel 17. Den dataansvarlige vil formentlig i et sådan tilfælde kunne gennemføre passende tekniske og organisatoriske foranstaltninger med mindre omfattende tiltag end databeskyttelsespolitikker vedrørende retten til at blive glemt.

Udover at vurdere, hvilke foranstaltninger, der kan anses for passende i forhold til den konkrete behandlingsaktivitet, skal den dataansvarlige desuden efter artikel 24, stk. 1, være i stand til at påvise, at behandlingen er i overensstemmelse med forordningen. Dermed skal

[501] Artikel 29-gruppens udtalelse nr. 173/2010 om princippet om ansvarlighed (WP), s. 11ff.

den dataansvarlige kunne påvise over for interne såvel som eksterne interessenter, såsom tilsynsmyndighederne, at de valgte og gennemførte foranstaltninger er effektive, således at de pågældende behandlingsaktiviteter rent faktisk overholder forordningens regler. Det er derfor ikke nok til at efterleve forpligtelserne efter artikel 24, stk. 1, at denne blot gennemfører passende tekniske og organisatoriske foranstaltninger uden løbende at følge op på, om disse rent faktisk er effektive.

Artikel 29-gruppen foreslår i sin udtalelse om princippet om ansvarlighed, at dataansvarlige ved beslutning om, hvordan foranstaltningernes effektivitet skal sikres, skal anvende de risici, som behandlingen indebærer samt oplysningernes art, som kriterier for disse.[502] I tilfælde af større, mere komplekse eller risikobetonede databehandlinger bør det således regelmæssigt kontrolleres, at de vedtagne foranstaltninger er effektive, f.eks. ved at vurdere effektiviteten ved interne eller eksterne revisioner, overvågning mv. Ved mindre risikobetonede behandlingsaktiviteter, kan det formentlig være nok med en løbende og mindre omfattende evaluering af de gennemførte foranstaltninger mv.

Som et element til at påvise, at den dataansvarlige overholder sine forpligtelser efter artikel 24, stk. 1, kan denne som følge af forordningens artikel 24, stk. 3, bruge overholdelsen af godkendte adfærdskodekser efter forordningens artikel 40 eller godkendte certificeringsmekanismer efter artikel 42. Disse kodekser og mekanismer vil således kunne bidrage til at bevise, at den dataansvarlige overholder sit ansvar efter artikel 24, stk.1, og at denne derfor har defineret og gennemført passende foranstaltninger, som jævnligt er blevet revideret.[503] Det må antages, at kodekser og mekanismer, som følge af bestemmelsens ordlyd, ikke kan stå alene i den dataansvarliges bevis for, at dennes behandlingsaktiviteter overholder forordningens regler. Der henvises til særskilt afsnit om databeskyttelsesforordningens artikel 40 og 42.

I forhold til gældende ret, er der ikke noget nyt i, at der efter forordningens artikel 24 stilles krav om, at den dataansvarlige skal efterleve de databeskyttelsesretlige regler. Størstedelen af de krav, som stilles til den dataansvarlige efter bestemmelsen findes således allerede i gældende lovgivning, om end mindre eksplicit. Udover kravet om, at den dataansvarlige skal kunne påvise at dennes behandling er i overensstemmelse med forordningen, pålægges den dataansvarlige således ikke krav, som ikke allerede implicit findes i gældende lovgivning.

[502] Artikel 29-gruppens udtalelse nr. 173/2010 om princippet om ansvarlighed (WP), s. 15.
[503] Artikel 29-gruppens udtalelse nr. 173/2010 om princippet om ansvarlighed (WP), s. 18.

5.1.4. Overvejelser

Artikel 24 i den generelle databeskyttelsesforordning om den dataansvarliges ansvar indeholder i høj grad forpligtelser for den dataansvarlige, der allerede implicit følger af gældende ret. Nyskabelsen består i, at den dataansvarliges ansvar eksplicit beskrives i forordningen, og at den dataansvarlige er forpligtet til at være i stand til at påvise, at denne overholder sit ansvar efter forordningen. Forordningens artikel 24 ses således i høj grad at have samme indhold som gældende ret.

5.2. Databeskyttelse gennem design og standardindstillinger, artikel 25

5.2.1. Præsentation

Databeskyttelsesforordningens artikel 25 fastsætter principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

Forordningens artikel 25 skal ses i sammenhæng med de øvrige bestemmelser i forordningen, herunder særligt artikel 5 om principper for behandling, artikel 32 om behandlingssikkerhed samt artikel 35 om konsekvensanalyse.

Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger vedrører helt overordnet, hvordan den dataansvarlige skal indrette sig teknisk og organisatorisk for at opnå effektiv implementering af databeskyttelsesprincipper og integrere de fornødne garantier i behandlingen for at opfylde kravene i databeskyttelsesforordningen og beskytte de registreredes rettigheder.

Hverken databeskyttelsesdirektivet eller persondataloven indeholder bestemmelser, som specifikt kræver databeskyttelse gennem design eller databeskyttelse gennem standardindstillinger. Der findes således ikke i gældende ret en bestemmelse, som svarer direkte til databeskyttelsesforordningens artikel 25. Bestemmelsens område er dog dækket af flere bestemmelser i gældende ret, hvorfor disse vil blive omtalt i det følgende.

5.2.2. Gældende ret

5.2.2.1. Databeskyttelsesdirektivet

Selvom databeskyttelsesdirektivet ikke indeholder en bestemmelse, der er direkte sammenlignelig med forordningens artikel 25, er begreberne databeskyttelse gennem design og indstillinger ikke ukendte fænomener.

Artikel 29-gruppen har i den henseende bl.a. udtalt, at databeskyttelsesdirekivet indeholder flere bestemmelser, som opfordrer de dataansvarlige til at gennemføre teknologibeskyttel-

sesregler i forbindelse med både design og drift af informations- og kommunikations teknologier.[504] Artikel 29-gruppen nævner bl.a. direktivets artikel 17, hvor der fastsættes en forpligtelse for den dataansvarlige til at gennemføre passende tekniske og organisatoriske foranstaltninger.

Databeskyttelsesdirektivets artikel 17 forpligter således medlemsstaterne til at fastsætte bestemmelser om, at den dataansvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for ulovlig behandling. Bestemmelsen er implementeret i dansk ret ved persondatalovens § 41, stk. 3.

Beskyttelsen skal iværksættes af den dataansvarlige ved hjælp af de fornødne tekniske og organisatoriske foranstaltninger.

Foranstaltningerne skal tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse.

Herudover nævner Artikel 29-gruppen direktivets præambelbetragtning nr. 46, hvoraf fremgår, at foranstaltningerne skal træffes både under selve udformningen og under iværksættelsen af en behandling. Det fremgår af den engelske version af præambelbetragtningen, at: *"appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself"*. Anvendelsen af ordet *udformningen* i den danske betragtning findes således at være knyttet til "udformningen af behandlingssystemet".

Bestemmelsen i direktivet må antages at skulle fortolkes således, at en dataansvarlig eksempelvis skal sikre sig, at personoplysninger ikke ubeføjet udbredes eller på anden vis kompromitteres, f.eks. gennem en utilsigtet offentliggørelse af personoplysninger på internettet, utilstrækkelig beskyttelse af uddatamateriale eller mangelfuld opsætning af IT-systemer. Organisatorisk skal den dataansvarlige eksempelvis sikre, at oplysninger ikke kommer til uvedkommendes kendskab. En "clean-desk"-policy kan være en måde at forebygge, at det øvrige personale eksempelvis bliver bekendt med afskedigelsespapirer, som en HR-ansvarlig kan have liggende på sit bord.

[504] Artikel 29-gruppens udtalelse om "The Future of Privacy", vedtaget den 1. december 2009, (WP 168), s. 13, nr. 44.

I relation til de mere tekniske foranstaltninger udtaler Artikel 29-gruppen generelt om begrebet "indbygget privatlivsbeskyttelse" i en udtalelse om apps i intelligente enheder, at begrebet "indbygget privatlivsbeskyttelse" ("privacy by design") er et vigtigt princip, som allerede indirekte blev nævnt i databeskyttelsesdirektivet, navnlig i artikel 17 og præambelbetragtning nr. 46, og som sammen med "privatlivsbeskyttelse som standard" ("privacy by default") kommer mere klart frem i e-databeskyttelsesdirektivet.[505]

Artikel 29-gruppen anfører endvidere i udtalelsen, at for at kunne opfylde de respektive sikkerhedsforpligtelser som dataansvarlige skal app-udviklere, app-butikker, OS- og enhedsproducenter og tredjeparter tage højde for principperne om indbygget privatlivsbeskyttelse og privatlivsbeskyttelse som standard. Artikel 29-gruppen henviser i den forbindelse igen til direktivets artikel 17. Dette kræver ifølge Artikel 29-gruppen løbende vurdering af både eksisterende og fremtidige databeskyttelsesrisici samt gennemførelse og evaluering af effektive afbødende foranstaltninger, herunder dataminimering.[506] Overholdelse af sikkerhedspligten har således ifølge Artikel 29-gruppen et dobbelt formål. Det giver brugerne mulighed for at føre strengere kontrol med deres oplysninger og styrker tilliden til de enheder, der håndterer brugernes oplysninger.

5.2.2.2. Persondataloven

Persondatalovens krav til behandling af personoplysninger skal iagttages f.eks. ved indretningen af IT-løsninger og fastlæggelse af arbejdsgange. I denne sammenhæng har navnlig behandlingsbetingelserne i lovens kapitel 4 og kravene til datasikkerheden i lovens § 41, stk. 3, betydning.

Det bemærkes, at det følger af persondatalovens generelle databehandlingsprincipper i § 5, at indsamling og senere behandling af personoplysninger skal ske til udtrykkeligt angivne og saglige formål. Det fremgår endvidere, at oplysningerne skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil de er indsamlet. Bestemmelsen stiller ligeledes krav om, at indsamlede oplysninger ikke opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til formålet med behandlingen. Disse behandlingsprincipper er generelle og gælder for al behandling af personoplysninger, det vil sige både for den organisatoriske tilrettelæggelse af behandlinger og for indretningen af IT-systemer.

[505] Artikel 29-gruppens udtalelse nr. 02/2013 om apps i intelligente enheder (WP 202), afsnit 3.2.2 OS- og enhedsproducenter.
[506] Artikel 29-gruppens udtalelse nr. 02/2013 om apps i intelligente enheder, (WP 202), afsnit 3.6 Sikkerhed.

Persondatalovens § 41, stk. 3, der implementerer direktivets artikel 17, stk. 1, forpligter den dataansvarlige og databehandleren til at træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven.

Det gør sig gældende både, når systemet er idriftsat, men også tidligere eksempelvis i testfasen.

Offentlige myndigheder er endvidere i dag forpligtet til at indrette sig i overensstemmelse med sikkerhedsbekendtgørelsen, som har hjemmel i persondatalovens § 41, stk. 5. Sikkerhedsbekendtgørelsen indeholder to sikkerhedsniveauer, hvilket betyder, at kravene i kapitel 3 alene finder anvendelse i forbindelse med behandling af anmeldelsespligtige oplysninger.

Autorisation, logning og tilvejebringelse af medarbejderinstrukser er blandt de krav, der stilles til de offentlige myndigheder i sikkerhedsbekendtgørelsen. Disse tekniske og organisatoriske foranstaltninger beror ikke på en risikovurdering, men kræves truffet, uanset hvordan myndigheden i øvrigt er indrettet.

Udover at være sikkerhedsforanstaltninger kan visse dele af sikkerhedsbekendtgørelsen, såsom f.eks. adgangsbegrænsning, anses for eksempler på databeskyttelse gennem design og standardindstillinger.

Det forhold, at de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger også skal sikre overholdelse af de øvrige regler i persondataloven, udover reglerne i § 41, stk. 3, og sikkerhedsbekendtgørelsen, fremgår af Datatilsynets udtalelse vedrørende en høring i Den Tværoffentlige Arbejdsgruppe vedrørende Privacy.[507] Her udtalte Datatilsynet, at der ved test i forbindelse med program- og systemudvikling bør anvendes egentlige testdata, dvs. oplysninger om fiktive personer, og ikke oplysninger om eksisterende personer. Der bør således ikke som testdata anvendes kopi af produktionsdata, medmindre der forinden er foretaget en effektiv anonymisering af disse.

Det fremgår af persondataloven med kommentarer, at de fornødne tekniske og organisatoriske foranstaltningerne efter § 41, stk. 3, skal træffes på baggrund af de hensyn, der fremgår af direktivets artikel 17, stk. 1, 2. afsnit.[508]

[507] Datatilsynets udtalelse vedrørende en høring i Den Tværoffentlige Arbejdsgruppe vedrørende Privacy, Datatilsynets j.nr. 2007-081-0011.
[508] Persondataloven med kommentarer (2015), s. 548.

Persondataloven fastsætter ingen nærmere tidsmæssig ramme for, hvornår de fornødne tekniske og organisatoriske foranstaltningerne skal være truffet. Foranstaltningerne vil dog skulle forberedes og implementeres forud for, at behandlingen påbegyndes – det vil sige også i testfasen, som det fremgår af Datatilsynets udtalelse ovenfor. Der findes dog foranstaltninger, som først kan træffes efter behandlingen, som eksempelvis fuld test af back-up systemerne. Når foranstaltningerne træffes forud for behandlingen, vil det tillige være i overensstemmelse med direktivets præambelbetragtning nr. 46, som nævnes ovenfor.

Det fremgår af Center for Cybersikkerhed og Digitaliseringsstyrelsens anbefalinger til styrkelse af sikkerheden i statens outsourcede IT-drift[509], at reglerne i persondataloven og den tilhørende sikkerhedsvejledning skal iagttages, inden behandlingen af personoplysninger starter.[510]

Persondatalovens § 41, stk. 3, fastsætter endvidere, at foranstaltningerne blandt andet skal sikre mod, at oplysningerne behandles i strid med loven. Dette indebærer, at de tekniske og organisatoriske foranstaltninger skal sammenholdes med lovens øvrige regler.

Der findes i Datatilsynets praksis en del eksempler på, at både persondatalovens behandlingsbetingelser, herunder eksempelvis legalitetsprincippet og de registreredes rettigheder samt sikkerhedskrav, skal iagttages ved indretningen af digitale løsninger.

Der kan bl.a. henvises til Datatilsynets udtalelse i en sag om en hjemmeside, hvor brugerne havde mulighed for at oprette en personlig helbredsboks med adgang til bl.a. helbredsoplysninger fra læger.[511] I denne sag udtalte Datatilsynet, at den anvendte løsning med login baseret på brugernavn og adgangskode ikke i tilstrækkelig grad levede op til den sikkerhed, som må kræves, når en hjemmeside som den i sagen omhandlede gav adgang til følsomme personoplysninger på sundhedsområdet.

Datatilsynet opfordrede endvidere i et høringssvar[512] vedrørende et lovforslag fra Digitaliseringsstyrelsen om obligatorisk selvbetjening (”bølge 3”) til, at man udformede de omhandlede løsninger og forretningsgange således, at borgerne kunne stole på, at data til enhver tid var beskyttet. I den forbindelse understregede Datatilsynet generelt behovet for, at der ved udviklingen af løsningen var fokus på beskyttelsen af personoplysninger og privatliv samt efterlevelse af persondataloven. Beskyttelsen af personoplysninger og privatliv burde derfor efter tilsynets opfattelse indgå som en integreret del af systemudviklingen.

[509] Rapporten er den tredje om CSC-sagen, som blev bestilt af regeringen i sommeren 2013 og udarbejdet af Center for Cybersikkerhed og Digitaliseringsstyrelsen, 6. januar 2017.
[510] Anbefalinger til styrkelse af sikkerheden i statens outsourcede IT-drift, s. 15, 2. spalte.
[511] Datatilsynets j.nr. 2015-631-0108.
[512] Datatilsynets j.nr. 2013-112-0268.

Datatilsynet anførte således, at der med andre ord skulle anvendes "Privacy by Design". I den forbindelse pegede Datatilsynet endvidere på brugen af privatlivsfremmende teknologier eller "Privacy Enhancing Technologies". Datatilsynet pegede desuden på behovet for at give borgerne ret til selvbestemmelse, hvor det er relevant. Endelig påpegede Datatilsynet vigtigheden af, at det er transparent for brugerne, hvilke data der behandles, og eventuelt tillige, hvem der anvender oplysningerne.

Folketingets Ombudsmand har om SKAT's EFI-system udtalt, at "det er et grundlæggende krav, at IT-systemer kan understøtte en korrekt anvendelse af relevant lovgivning, og dette kan i sagens natur klart bedst sikres ved en tilstrækkelig tidlig identifikation og systemindarbejdelse af de pågældende regelsæt." [513]

I praksis medfører persondataloven, at den dataansvarlige blandt andet skal træffe de fornødne tekniske og organisatoriske foranstaltninger for at sikre at de oplysninger, som behandles, er relevante og tilstrækkelige og ikke omfatter mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne blev indsamlet, og de formål, hvortil oplysningerne senere behandles i overensstemmelse med lovens § 5, stk. 2.

Tekniske foranstaltninger kan blandt andet rumme de så kaldte *Privacy Enhancing Techonologies* (PET's). Begrebet dækker generelt alle teknologier, som fremmer privatlivsbeskyttelse. Implementering af PET's kan afhjælpe den konkrete tekniske overholdelse af nogle af sikkerhedsforpligtelserne.

Kommissionen behandlede emnet om bl.a. PET's i deres meddelelse *om bedre databeskyttelse med teknologier til beskyttelse af privatlivet* i 2007.[514] I meddelelsen anfører Kommissionen blandt andet, at udover at fremme formålene med reglerne i chartrets artikel 8 om beskyttelse af personoplysninger og databeskyttelsesdirektivet ved at indskrænke behandlingen af personoplysninger, og hvor det er muligt, benytte anonyme eller pseudonyme oplysninger, kan der navnlig benyttes de såkaldte teknologier til beskyttelse af privatlivet (PET's).

Kommissionen anførte endvidere i meddelelsen, at der ved hjælp af PET's kan udformes informations- og kommunikationssystemer og tjenesteydelser, hvor indsamling og anvendelse af personoplysninger kan indskrænkes, og hvor det er lettere at overholde databeskyttelsesreglerne.[515] Kommissionen bemærker i øvrigt, at det med disse teknologier til beskyt-

[513] Ombudsmandens sag nr. 2014-24, s. 2.
[514] Meddelelse fra kommissionen til Europa-Parlamentet og Rådet om bedre databeskyttelse med teknologier til beskyttelse af privatlivet, KOM (2007) 228 endelig.
[515] Kommissionens meddelelse, KOM (2007) 228 endelig, afsnit 2., s. 3.

telse af privatlivet skulle blive vanskeligere at krænke visse databeskyttelsesregler samtidig med, at det skulle blive lettere at opspore krænkelser.

Herudover kan der henvises til publikationen "privacy and Data Protection by Design – from policy to enginerring", som ENISA udgav i 2014, og som indeholder relevant vejledning, ligesom den daværende IT- og Telestyrelses udgivelse fra januar 2011 "Nye digitale sikkerhedsmodeller" kan anvendes som vejledning. Materialet kan således vejlede den dataansvarlige, når denne skal træffe de fornødne tekniske og organisatoriske foranstaltninger.

5.2.3. Databeskyttelsesforordningen

Databeskyttelsesforordningens artikel 25 forpligter helt overordnet den dataansvarlige til at træffe passende tekniske og organisatoriske foranstaltninger, som er designet og præindstillet med henblik på at opfylde kravene i forordningen og beskytte de registreredes rettigheder. Bestemmelsen indebærer, at der for behandlingen som helhed skal træffes både tekniske og organisatoriske foranstaltninger. Der er imidlertid ikke krav om, at der træffes både tekniske og organisatoriske foranstaltninger for hvert enkelt delelement i behandlingen.

5.2.3.1. Databeskyttelsesforordningens artikel 25, stk. 1, databeskyttelse gennem design

Det fremgår af artikel 25, stk. 1, at den dataansvarlige forpligtes til at opfylde kravene i forordningen og beskytte de registreredes rettigheder ved gennemførelse af passende tekniske og organisatoriske foranstaltninger, som er *designet* med henblik på *effektiv implementering af databeskyttelsesprincipper og med henblik på integrering af de fornødne garantier i behandlingen af personoplysninger for at opfylde kravene i forordningen og beskytte de registreredes rettigheder.*

Begrebet "databeskyttelse gennem design" må efter ordlyden forstås bredt, således at det omfatter både tekniske og organisatoriske foranstaltninger. Design må derfor antages at omfatte både et middel, eksempelvis et IT-systems tekniske indretning og brugergrænseflade, samt den måde den dataansvarlige organisatorisk er indrettet på.

I modsætning til efter gældende ret er der med forordningens artikel 25, stk. 1, et eksplicit krav om databeskyttelse gennem design.

På baggrund af ordlyden i artikel 25, stk. 1, skal foranstaltningerne gennemføres både på "tidspunktet for fastlæggelse af midlerne til behandling" (forberedelsesfasen) og "på tidspunktet for selve behandlingen". Sidstnævnte tidspunkt må antages at betyde den første dag, behandlingen begynder.

Forordningens artikel 25, stk. 1, må antages at indebære en *overvejelsesforpligtelse* og en *håndteringsforpligtelse* for den dataansvarlige til allerede i forberedelsesfasen at indtænke de relevante foranstaltninger til sikring af overholdelse af databeskyttelsesforordningen.

Efter artikel 25, stk. 1, skal der gennemføres passende tekniske og organisatoriske foranstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer.

Det skal hertil bemærkes, at forordningens artikel 25, stk.1, er udtryk for en risikobaseret tilgang til databeskyttelse, og bestemmelsen angiver kun ganske overordnede retningslinjer for, hvilke typer af tiltag bestemmelsen sigter mod. Dette indebærer, at den dataansvarlige overlades et ganske væsentligt råderum, inden for hvilket denne har adgang til at vurdere og fastlægge, hvilke foranstaltninger der konkret bør implementeres for at efterleve bestemmelsen.

Artikel 25, stk. 1, må antages at indebære en pligt for den dataansvarlige til at inddrage tiltag, der konkret fremmer en effektiv implementering af forordningens databeskyttelsesprincipper i artikel 5 og dens øvrige regler.

Dermed skal den dataansvarlige overveje og håndtere, hvordan databeskyttelse generelt, dvs. alle forordningens bestemmelser, kan efterleves med konkrete foranstaltninger i *design* af IT-systemer, såsom deres tekniske indretning og brugergrænseflade, samt ved *indretningen* af den dataansvarliges organisation.

Et eksempel på en situation, hvor denne afvejning af hensyn kommer i fokus, vil være, når et ældre systems sikkerhed skal gennemgås. Viser det sig i et sådant tilfælde, at systemet ikke på alle områder helt modsvarer det aktuelle tekniske niveau[516], men at implementeringsomkostningerne ved at bringe hele systemet på niveau er uforholdsmæssigt store, kan den dataansvarlige i stedet søge at imødekomme behovet for større sikkerhed ved hjælp af også organisatoriske foranstaltninger. Der er således ingen forpligtelse til at efterkomme sikkerhedskravene alene rent teknisk, såfremt der efter en konkret vurdering fra den dataansvarlige findes tilstrækkelige organisatoriske løsninger, der også kan bidrage til at sikre det aktuelle tekniske niveau.

[516] Begrebet skal forstås i overensstemmelse med den engelske sprogversion, hvor der står "*state of the art"*. "*Det aktuelle niveau"* forstås derfor som *"det højest mulige niveau"*.

Kan der etableres et passende sikkerhedsniveau for allerede ibrugtagne ældre systemer også gennem interne procedurer, undervisning af ansatte eller tilsvarende organisatoriske foranstaltninger, vil dette i princippet kunne være tilstrækkeligt.

Forordningens artikel 25, stk. 1, medfører med andre ord ikke et krav om, at eksempelvis ældre systemer skal re-designes, hvis der eksempelvis findes organisatoriske sikkerhedsløsninger, der må anses for tilstrækkelige. Dette skyldes, at forordningen først finder anvendelse den 25. maj 2018, og at artikel 25, stk. 1, således ikke finder anvendelse på allerede eksisterende systemer, jf. ordlyden i artikel 25, stk. 2: "tidspunktet for fastlæggelse" og "tidspunktet for selve behandlingen". Andre bestemmelser såsom artikel 32 om behandlingssikkerhed og artikel 5 kan dog medføre krav om ændringer efter den 25. maj 2018, såfremt det eksisterende system ikke overholder forordningen.

Eksempler på foranstaltninger, der efterlever principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, følger af præambelbetragtning nr. 78, hvoraf det fremgår, at sådanne foranstaltninger bl.a. kan bestå i minimering af behandlingen af personoplysninger, pseudonymisering af personoplysninger så hurtigt som muligt og gennemsigtighed for så vidt angår personoplysningers funktion og behandling, således at den registrerede kan overvåge databehandlingen, og den dataansvarlige kan tilvejebringe og forbedre sikkerhedselementer.

Pseudonymisering og dataminimering nævnes endvidere i artikel 25, stk. 1, som eksempler på henholdsvis en foranstaltning og et databeskyttelsesprincip, der kan iagttages. Pseudonymisering er nærmere defineret i forordningens artikel 4, nr. 5, mens dataminimeringsprincippet fremgår af artikel 5, stk. 1, litra c.

Referencen til eksempelvis dataminimering i artikel 25, stk. 1, er ligeledes ikke udtryk for, at der skal foretages en anden vurdering end i dag af, hvorvidt de oplysninger der allerede er i f.eks. et IT-system, bør være der. Idet forordningens artikel 5 om principper for behandling af personoplysninger som udgangspunkt er en videreførelse af gældende ret, vil den lovlige behandling af de personoplysninger, de enkelte dataansvarlige har i deres systemer, også være berettiget, når forordningen finder anvendelse, såfremt behandlingen i øvrigt er lovlig efter forordningens øvrige bestemmelser.

Blandt de foranstaltninger, som en dataansvarlig i hvert fald må antages at være forpligtet til at implementere, må være en sikring af, at de midler – f.eks. et IT-system – der bringes i anvendelse, medvirker til en efterlevelse af forordningens øvrige krav. Dette følger af kravet i artikel 25, stk. 1, om, at de fornødne sikkerhedsforanstaltninger skal "opfylde kravene i denne forordning".

Udvikler den dataansvarlige selv systemerne, vil dette kunne afhjælpes ved bl.a. at indarbejde *Privacy Enhancing Tehcnologies* (PET's).

Køber den dataansvarlige et IT-system eller en IT-løsning, kan den dataansvarlige forsøge at løfte opgaven kontraktuelt ved at stille krav om, at systemet bygges i overensstemmelse med relevante bestemmelser i forordningen. Dette fritager dog ikke den dataansvarlige for ansvar og forpligtelser i henhold til forordningen. For offentlige myndigheder vil denne opgave typisk ligge i udbudsfasen i overensstemmelse med anvisningen i præambelbetragtning nr. 78, hvoraf det følger, at der også bør tages hensyn til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i forbindelse med offentlige udbud.

I forbindelse med udbud af IT-løsninger kan kunden (myndigheden, organisationen, virksomheden osv.) eksempelvis vælge at angive i kravspecifikationen, hvilke PET's der kunne ønskes anvendt i den kommende IT-løsning. Kunden kan endvidere vælge i kravspecifikationen at præcisere sikkerhedskravene til testmiljøet. Endelig kan kunden vælge at eksemplificere kravene i myndighedens informationssikkerhedspolitik mv.

Som eksempel på relevante bestemmelser i forordningen, som endvidere udtrykkeligt efter ordlyden af artikel 25, stk. 1, skal inddrages, er forordningens bestemmelser om de registreredes rettigheder.

Efter omstændighederne vil design af et IT-system omfattet af artikel 25, stk. 1, der *ikke* sikrer, at den registreredes anmodning om f.eks. indsigt (artikel 15), ret til dataportabilitet (artikel 20) eller ret til begrænsning af behandling (artikel 18), kan imødekommes, således kunne udgøre en overtrædelse af forpligtelsen til databeskyttelse gennem design i artikel 25, stk. 1.

Det må dog antages, at en sådan situation delvist vil kunne afhjælpes ved implementering af organisatoriske foranstaltninger, der gør den registrerede i stand til at gøre sin ret til indsigt gældende. For eksempel vil en dataansvarlig, der sjældent modtager anmodninger om indsigt, således ikke være forpligtet – som standard – til at indkøbe et nyt IT-system for at kunne imødekomme anmodninger fra de registrerede rent teknisk, i det omfang anmodningerne kan imødekommes ved hjælp af organisatoriske foranstaltninger.

Artikel 25, stk. 1, indebærer endvidere, at den dataansvarlige blandt andet skal anvende foranstaltninger, der er designet med henblik på effektiv implementering af databeskyttelsesprincipper og med henblik på integrering af de fornødne garantier i behandlingen. Begrebet *garantier* i forordningens artikel 25, stk. 1, skal også forstås i overensstemmelse

med den engelske sprogversion, hvor der skrives *safeguards*, hvilket i denne sammenhæng kan forstås som "værn" eller "beskyttelse".

Der er ikke nærmere redegjort for betydningen af begrebet *databeskyttelsesprincipper* i artikel 25, men forordningens artikel 5 indeholder en opregning af disse. Artikel 5 angiver således konkret principperne om formålsbegrænsning, dataminimering, begrænsede opbevaringsperioder, datakvalitet, retsgrundlag for behandling, behandling af særlige kategorier af personoplysninger, foranstaltninger til at sikre datasikkerhed og krav til videreoverførsel. Det bemærkes, at den dataansvarlige efter artikel 5 er forpligtet til at efterleve disse principper i enhver behandling af personoplysninger.

Endelig skal det bemærkes, at artikel 25, stk. 1, bør ses i sammenhæng med artikel 35 om konsekvensanalyse vedrørende databeskyttelse. Gennemførelsen af en konsekvensanalyse skaber mulighed for – på et bevidst og oplyst grundlag – at designe tekniske privatlivsbeskyttende løsninger ind i systemet fra start.

5.2.3.2. Databeskyttelsesforordningens artikel 25, stk. 2, databeskyttelse gennem standardindstillinger

Forordningens artikel 25, stk. 2, fastsætter princippet om databeskyttelse gennem *standardindstillinger*. Bestemmelsen foreskriver, at den dataansvarlige skal sikre, at det kun er de personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, der bliver behandlet. Det skal også sikres, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.

Standardindstillinger skal efter ordlyden af artikel 25, stk. 2, forstås bredt, således at det omfatter både tekniske og organisatoriske foranstaltninger. Standardindstillinger kan derfor forstås som både IT-tekniske indstillinger og de almene forretningsgange, som understøtter databeskyttelse, herunder eksempelvis, at adgang til personoplysninger – analoge såvel som digitale – er arbejdsbetingede og ikke lige tilgængelige for alle i den dataansvarliges organisation.

I modsætning til efter gældende ret er der derfor med forordningen et eksplicit krav om at overveje databeskyttelse gennem standardindstillinger, såfremt det er muligt. Opgaven skal løses gennem standardindstillinger på basis af passende tekniske og organisatoriske foranstaltninger.

Til forskel fra bestemmelsen i artikel 25, stk. 1, der vedrører selve designfasen, ses artikel 25, stk. 2, at udtrykke en pligt for den dataansvarlige til at sikre, at når f.eks. et softwareprogram, en online tjeneste, et IT-system eller lignende anvendes til at behandle personop-

lysninger, skal de indstillingsmuligheder, som systemet mv. indeholder, som standard indstilles på en måde, der understøtter bestemmelsens krav om bl.a. formålsspecifik behandling af personoplysninger.

Dette krav må eksempelvis indebære, at første gang en tjeneste, f.eks. en online tjeneste, en app eller et stykke software, stilles til rådighed for en given bruger eller medarbejder, skal de relevante indstillinger, der vedrører behandlingen af personoplysninger i forbindelse med brugen af tjenesten, i overensstemmelse med dataminimeringsprincippet i artikel 5, stk. 1, litra c, som standard indebære den mindst mulige deling af personoplysninger.

Kravet i artikel 25, stk. 2, kan således ses som en "tilføjelse" til kravet om databeskyttelse gennem design i artikel 25, stk. 1, idet stk. 1 konkret kan indebære, at et system designes med særlige databeskyttelsesfremmende indstillinger indbygget, og bestemmelsen i artikel 25, stk. 2, pålægger således den dataansvarlige f.eks. at gøre den mest formålsbegrænsende indstilling af systemet til standardindstillingen.

For så vidt angår systemer, der er tilvejebragt inden den 25. maj 2018, som er indrettet i overensstemmelse med gældende ret, vil artikel 25, stk. 2, ikke umiddelbart medføre, at eksisterende systemer skal ændres. Det skal dog bemærkes, at såfremt det er *muligt* at ændre i standardindstillingerne i et system, der er tilvejebragt inden den 25. maj 2018, vil disse skulle ændres i overensstemmelse med artikel 25, stk. 2.

I det omfang et systems indstillinger skal ændres for at kunne overholde de krav, der i øvrigt følger af forordningen, herunder eksempelvis artikel 5, kapitel III om den registreredes rettigheder og artikel 32, er den dataansvarlige dog forpligtet til at ændre disse indstillinger, så det lever op til forordningens artikel 25, stk. 2, fra den 25. maj 2018.

Kravet i forordningens artikel 25, stk. 2, 1. pkt., kan endvidere antages at betyde, at når en fysisk person eksempelvis downloader en app på en smartphone, et smartwatch, en fitness tracker eller et digitaliseret legetøj, skal den dataansvarlige, der er ansvarlig for behandlingen af personoplysninger, gennem standardindstillinger sikre, at der ikke bliver indsamlet flere oplysninger, end nødvendigt for at opnå formålet med app'en.

Det kan desuden antages, at artikel 25, stk. 2, indebærer, at en sådan app – i det omfang forholdet er regulerbart gennem standardindstillinger – ikke må have standardindstillinger, der gør, at der deles oplysninger om eksempelvis, at en person har været på en bestemt beværtning, løbet en tur eller hvem vedkommende har været sammen med, medmindre denne deling er selve formålet med app'en.

Hvis deling af personoplysninger *ikke* er regulerbart gennem standardindstillinger i app'en, kan det være tegn på manglende efterlevelse af artikel 25, stk. 1, idet det kan skyldes, at den dataansvarlige ikke har sikret databeskyttelse gennem design i app'en.

Forordningens artikel 25, stk. 2, 2. pkt. fastslår endvidere udtrykkeligt, at de behandlede personoplysninger ikke uden den pågældende persons indgriben må stilles til rådighed for et ubegrænset antal fysiske personer. Dette må bl.a. antages at sigte mod, at systemer eller tjenester, der giver fysiske personer adgang til at oprette profiler på online-platforme, kun må lade personoplysninger være tilgængelige for et ubegrænset antal fysiske personer, på baggrund af den pågældende persons egen konkrete indgriben.

5.2.3.3. Databeskyttelsesforordningens artikel 25, stk. 3, godkendte certificeringsmekanismer

Forordningens artikel 25, stk. 3, giver mulighed for, at der kan anvendes *godkendte certificeringsmekanismer* efter forordningens artikel 42 som et element til at påvise overholdelse af kravene om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Certificering efter en godkendt certificeringsmekanisme i medfør af artikel 42, kan imidlertid ikke stå alene som bevis for overholdelse af forordningens krav.

5.2.4. Overvejelser

Databeskyttelsesforordningens artikel 25 etablerer ikke i sig selv nye krav til den dataansvarlige, idet kravene i artikel 25 om bl.a. passende tekniske og organisatoriske foranstaltninger, dataminimering, formålsspecifik behandling samt sikring af de registreredes rettigheder mv., allerede følger af gældende databeskyttelsesret, herunder databeskyttelsesdirektivets artikel 17 sammenholdt med direktivets præambelbetragtning nr. 46, sikkerhedsbekendtgørelsen, Artikel 29-gruppens udtalelser og Datatilsynets praksis.

Det er dog en nyskabelse, at databeskyttelse gennem design og standardindstillinger nævnes som en eksplicit forpligtelse for den dataansvarlige i forordningen.

Det er endvidere en nyskabelse med artikel 25, stk. 1, om databeskyttelse gennem design, at selve *tidspunktet* for, hvornår den dataansvarlige skal *overveje* og *håndtere*, hvilke foranstaltninger, der kan sikre efterlevelsen af alle databeskyttelsesreglerne i forordningen ved behandling af personoplysninger ændres.

Nyskabelsen i artikel 25, stk.1, består således i, at den dataansvarlige er forpligtet til at *overveje* og *håndtere*, hvorledes denne ved hjælp af tekniske og organisatoriske foranstaltninger kan sikre databeskyttelse gennem design for derved at efterleve reglerne i databeskyttelsesforordningen allerede på tidspunktet for fastlæggelse af midlerne til en given

behandling af personoplysninger, det vil sige i *forberedelsesfasen*, og på tidspunktet for selve behandlingen, dvs. *den første dag* af selve behandlingen af personoplysninger i IT-systemet.

Herudover er det en nyskabelse, at den dataansvarlige i medfør af artikel 25, stk. 2, hvor det er muligt, skal ændre i sine standardindstillinger til bl.a. at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål, behandles.

Afslutningsvis skal det understreges, at den dataansvarlige – uanset i hvilket omfang dennes behandling af oplysninger er omfattet af artikel 25, stk. 1 og 2 – under alle omstændigheder *skal* leve op til de øvrige krav i databeskyttelsesforordningen, herunder artikel 5 og forordningens bestemmelser om de registreredes rettigheder samt ikke mindst artikel 32 om behandlingssikkerhed. Der er således flere gode grunde til allerede fra "dag 1", hvor et IT-system går i luften at sikre, at systemet kan leve op til forordningen.

5.3. Fælles dataansvar, artikel 26

5.3.1. Præsentation

Formålet med artikel 26 om fælles dataansvar (delt dataansvar) i databeskyttelsesforordningen er at sikre, at eventuelle fælles dataansvarlige på en gennemsigtig måde fastsætter deres respektive ansvar for overholdelsen af de forpligtelser, som følger af forordningen.

5.3.2. Gældende ret

Efter gældende ret er spørgsmålet om fælles dataansvar ikke direkte reguleret i hverken databeskyttelsesdirektivet eller persondataloven. Det følger imidlertid af definitionen af begrebet "den dataansvarlige" i persondatalovens § 3, nr. 4, at dette kan være en fysisk eller juridisk person, offentlig myndighed institution eller ethvert andet organ, der alene eller *sammen med andre* afgør, til hvilket formål og med hvilke virkemidler der må foretages behandling af oplysninger.

Det følger ligeledes af behandlingsbegrebet i lovens § 3, nr. 2, at en behandling kan indebære en eller flere rækker af behandlinger. Efter gældende ret kan der således godt være et fælles dataansvar eller flere dataansvarlige i forbindelse med en behandling af personoplysninger.

Til trods for dette vil der ofte kun være én dataansvarlig i forbindelse med behandling af personoplysninger. Det skyldes, at det i praksis oftest alene er én aktør, som afgør til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

Inden der foreligger et fælles dataansvar, kræves det, at disse aktører *begge* har det umiddelbare ansvar for behandlingen og ikke mindst dispositionsretten over de oplysninger, som behandles. Andre tilfælde, hvor et sådan fælles dataansvar kan forekomme, kan for eksempel være mellem overordnede og underordnede myndigheder, for eksempel inden for skatteområdet eller politiet.[517] Efter Datatilsynets praksis, kan der endvidere være fælles dataansvar, når en behandling af personoplysninger drives i en enhed, som organisatorisk er forankret hos to forskellige virksomheder.[518]

Som udgangspunkt bør dataansvaret dog placeres hos én aktør, såsom én offentlig myndighed, privat virksomhed mv. Det skyldes bl.a., at det i tilfælde af flere dataansvarlige kan være svært at fastlægge, hvilken af de dataansvarlige der er kompetent – og ansvarlig – for de forpligtelser, som følger af persondataloven, når de forskellige dataansvarlige deler formål og hjælpemidler med behandlingen af oplysninger.[519] Der er således en risiko for, at der opstår en situation, hvor forpligtelser eller rettigheder ikke sikres af nogen af de fælles dataansvarlige.[520] Datatilsynet har også kun i enkelte og konkret begrundede sager accepteret, at der forelå et fælles dataansvar.[521]

Selve spørgsmålet om fordelingen af ansvar og forpligtelser for de fælles dataansvarliges er ikke reguleret direkte i gældende ret. I sager, hvor Datatilsynet har accepteret et fælles dataansvar, har tilsynet lagt til grund, at der skal foreligge klare retningslinjer og instruktionsbeføjelser for så vidt angår behandlingen af oplysninger. Herudover skal de registrerede kunne gøre deres rettigheder efter persondatalovens kapitel III, såsom retten til indsigt, oplysninger mv., gældende over for enhver af de fælles dataansvarlige.

Herudover har Artikel 29-gruppen[522] udtalt, at fælles dataansvar kan medføre uønskede kompleksiteter og eventuelt mangel på klarhed i forbindelse med tildeling af ansvar. Dette kan skabe en risiko for, at hele behandlingen bliver ulovlig på grund af mangel på gennemsigtighed, og at den overtræder princippet om retfærdig behandling. Ifølge Artikel 29-gruppen er det således i tilfælde af fælles dataansvar afgørende, at der er en klar fordeling af ansvar for opfyldelse af databeskyttelsesreglerne og for eventuelle brud på disse.

[517] Persondataloven med kommentarer (2015), s. 163.
[518] Sagen om FDB og Coop Danmark A/S' medlemsprogram, Datatilsynets j.nr. 2007-212-0042.
[519] Artikel 29-gruppen udtalelse nr. 169/2010 om begreberne "registeransvarlig" og "registerfører" (WP), s. 22ff.
[520] Artikel 29-gruppens udtalelse nr. 169/2010 om begreberne "registeransvarlig" og "registerfører" (WP), s. 23.
[521] Sagen om FDB og Coop Danmark A/S' medlemsprogram, Datatilsynets j.nr. 2007-212-0042.
[522] Artikel 29-gruppens udtalelse nr. 169/2010 om begreberne "registeransvarlig" og "registerfører" (WP), s. 23.

5.3.3. Databeskyttelsesforordningen

Som en nyskabelse i forhold til gældende ret, er spørgsmålet om fælles dataansvar eksplicit reguleret i databeskyttelsesforordningen. Det følger af forordningens artikel 26, stk. 1, at hvis to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til en behandling af oplysninger, skal disse anses for fælles dataansvarlige efter forordningen.

Der er ikke tale om en udvidelse af anvendelsesområdet for fælles dataansvar i forhold til gældende ret, idet det fortsat er afgørende for, om der er fælles dataansvar, at den dataansvarlige *sammen med andre* fastlægger, til hvilket formål og med hvilke virkemidler, der må foretages behandling af oplysninger. Dermed foreligger der alene et fælles dataansvar, hvis flere dataansvarlige *sammen* har det umiddelbare ansvar for behandlingen og ikke mindst dispositionsretten og ansvaret for de oplysninger, som behandles.

Det følger af præambelbetragtning nr. 79 i forordningen, at det er nødvendigt med en klar fordeling af ansvarsområderne i medfør af forordningen, bl.a. når der er tale om fælles dataansvar for at sikre en effektiv beskyttelse af de registreredes rettigheder og frihedsrettigheder samt tilsynsmyndighedernes kontrol og foranstaltninger. De fælles dataansvarlige skal således efter artikel 26, stk. 1, på gennemsigtig vis fastsætte deres respektive ansvar for overholdelse af de forpligtelser, der følger af forordningen, medmindre ansvaret er fordelt i henhold til EU- eller medlemsstaternes nationale lovgivning, som de dataansvarlige er underlagt.

Som eksempel på en sådan ordning mellem de fælles dataansvarlige, kan være en fordeling af, hvem der er ansvarlig for forpligtelsen til at foretage fortegnelse over behandlingsaktiviteter efter forordningens artikel 30.

Kravet om en gennemsigtig og klar ansvarsfordeling gælder især for så vidt angår de registreredes udøvelse af rettigheder og de dataansvarliges oplysningspligt efter forordningens artikel 13 og 14.
Det kan endvidere fastsættes i ordningen mellem de dataansvarlige, hvilken af de fælles dataansvarlige der skal fungere som kontaktpunkt i forhold til den registrerede, når denne skal udøve sine rettigheder i henhold til forordningen.

Det angives nærmere i artikel 26, stk. 2, hvad denne ordning mellem de fælles dataansvarlige skal indeholde. Ordningen skal således efter bestemmelsen på behørig vis afspejle de respektive roller, som hver af de fælles dataansvarlige har i den pågældende behandling af oplysninger. Endvidere skal de fælles dataansvarliges forhold til de registrerede afspejles i

ordningen. Desuden skal hovedindholdet i ansvarsfordelingen gøres tilgængeligt for de registrerede.

Kravene til selve ansvarsfordelingen ved fælles dataansvar må anses for at svare til de krav, der følger af gældende ret efter Datatilsynets praksis, hvorved der ved fælles dataansvar skal foreligge klare retningslinjer og instruktionsbeføjelser for så vidt angår behandlingen af oplysninger. Forskellen er blot, at kravene til fælles dataansvar nu fremgår direkte af forordningens ordlyd i artikel 26.

Dette gør sig ligeledes gældende for så vidt angår de registreredes mulighed for at udøve deres rettigheder ved fælles dataansvar efter artikel 26, stk. 1. Det følger således af artikel 26, stk. 3, at uanset hvordan de fælles dataansvarliges ansvarsfordeling er udformet, kan de registrerede fortsat gøre deres rettigheder i henhold til forordningen gældende over for enhver af de fælles dataansvarlige.

Det betyder, at selvom de fælles dataansvarlige indbyrdes har fastsat, at det alene er den ene part, der har kompetence til at imødekomme de registreredes rettigheder, kan den registrerede fortsat gøre et krav efter kapitel III gældende mod en anden af de fælles dataansvarlige.

Det bemærkes endelig, at overtrædelse af forordningens artikel 26 er strafbelagt, jf. forordningens artikel 83, stk. 4, litra a, jf. stk. 9.

5.3.4. Overvejelser

Den nye generelle databeskyttelsesforordnings artikel 26 om fælles dataansvar indeholder som nævnt regler, som i vidt omfang svarer til de krav, der stilles til fælles dataansvar efter gældende ret.

5.4. Repræsentanter, artikel 27

5.4.1. Præsentation

Formålet med kravet om at udpege en repræsentant efter databeskyttelsesforordningens artikel 27 er at skabe klarhed over for bl.a. de registrerede om, hvem der repræsenterer den dataansvarlige eller databehandleren i EU, når denne er etableret i et tredjeland, og de europæiske databeskyttelsesregler finder anvendelse på den pågældende behandling af personoplysninger.

5.4.2. Gældende ret

Det fremgår af persondatalovens § 4, stk. 3, nr. 1, at loven også gælder for en dataansvarlig, som er etableret i et tredjeland, hvis behandlingen af oplysninger sker under benyttelse af hjælpemidler, der befinder sig i Danmark, medmindre hjælpemidlerne kun benyttes med henblik på forsendelse af oplysninger gennem EU's område.

Dataansvarlige, som på den baggrund er omfattet af persondataloven, skal udpege en repræsentant, som er etableret i Danmark, jf. persondatalovens § 4, stk. 4.

Det fremgår af bemærkningerne til persondatalovens § 4, stk. 4, om repræsentanterne, at reglerne herom er af mere teknisk karakter. Det fremgår endvidere af bemærkningerne, at den valgte repræsentant har samme rettigheder og forpligtelser som den dataansvarlige.[523] Dette indebærer bl.a., at den udpegede repræsentant skal foretage anmeldelse til Datatilsynet efter reglerne i kapitel 12 og 13, ligesom den registrerede efter omstændighederne vil skulle have oplysning om den dataansvarliges repræsentants identitet, jf. §§ 28 og 29.

Det følger desuden af bestemmelsens ordlyd, at den registreredes mulighed for at foretage retslige skridt mod vedkommende dataansvarlig ikke berøres af, at der er udpeget en repræsentant. Det betyder, at den registrerede fortsat kan gøre et krav gældende mod den dataansvarlige, herunder et erstatningskrav, selvom denne har udpeget en repræsentant i Danmark.

Af persondatalovens § 4, stk. 5, følger det, at det påhviler den dataansvarlige skriftligt at underrette Datatilsynet om, hvem der er udpeget som repræsentant for den pågældende. Bestemmelsen må anses for at være en ordensforskrift, der tilsigter at lette Datatilsynets kontrolmuligheder.[524] Det er imidlertid tvivlsomt, om det er en forudsætning for, at behandlingen kan gennemføres lovligt, at der er afgivet skriftlig meddelelse til Datatilsynet, i tilfælde omfattet af persondatalovens § 4, stk. 3, nr. 1.[525]

5.4.3. Databeskyttelsesforordningen

I databeskyttelsesforordningen stilles der ligeledes krav om, at der i visse tilfælde skal udpeges en repræsentant for den dataansvarlige eller databehandleren. Det følger således af forordningens artikel 27, stk. 1, at der i de tilfælde – og kun i de tilfælde – hvor den dataansvarlige eller databehandleren ikke er etableret i EU, men forordningen alligevel finder

[523] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 4.
[524] Persondataloven med kommentarer (2015), s. 188.
[525] Persondataloven med kommentarer (2015), s. 188 og Peter Blume, Personoplysningsloven, 1. udgave (2000), s. 52.

anvendelse på grund af dens territoriale anvendelsesområde, jf. artikel 3, stk. 2, om bl.a. udbud af varer eller tjenester, skriftligt skal udpeges en repræsentant i EU.

I forhold til gældende ret udvides pligten til at udpege en repræsentant til også at omfatte databehandlere. Herudover ændres det geografiske krav til repræsentantens etablering ligeledes i forhold til gældende ret, idet forordningen alene stiller krav om, at den udpegede repræsentant er etableret i EU, og derfor ikke nødvendigvis skal være etableret i Danmark.

I henhold til definitionen af begrebet "repræsentant" i forordningens artikel 4, nr. 17, kan denne enten udgøre en fysisk eller juridisk person, som repræsenterer den dataansvarlige eller databehandleren, hvad angår deres respektive forpligtelser efter forordningen.

Det må således lægges til grund, at repræsentanten er underlagt de samme forpligtelser og rettigheder som den dataansvarlige og databehandleren. Den registrerede skal således i visse tilfælde, som følge af oplysningspligten i artikel 13 og 14, have oplysninger om repræsentantens identitet og kontaktoplysninger. Herudover er repræsentanten efter artikel 30, hvis det er relevant, forpligtet til at føre fortegnelse over behandlingsaktiviteter under dennes ansvar samt samarbejde med tilsynsmyndigheden efter forordningens artikel 31 mv.

I lighed med gældende ret, har den valgte repræsentant således samme rettigheder og forpligtelser, som den aktør, denne repræsenterer. I forhold til gældende ret, stilles der i forordningens artikel 27 alene krav om, at repræsentanten udpeges skriftligt. Der er således ikke en forpligtelse til at meddele tilsynsmyndigheden dette som efter gældende ret.

Det følger af præambelbetragtning nr. 80 til forordningen, at en repræsentant bør udføre sine opgaver i overensstemmelse med mandatet fra den dataansvarlige eller databehandleren. Repræsentanten skal i den forbindelse bl.a. samarbejde med de kompetente myndigheder med hensyn til enhver foranstaltning, der træffes for at sikre overholdelse af forordningen.

Efter forordningens artikel 27, stk. 2, litra a, gælder forpligtelsen til at udpege en repræsentant dog ikke lejlighedsvis behandling, som ikke i et stort omfang omfatter behandling af særlige kategorier af personoplysninger efter artikel 9, stk. 1, og oplysninger om straffedomme og lovovertrædelser efter artikel 10. Det skal samtidig være usandsynligt, at den pågældende behandling indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder under hensynstagen til behandlingens karakter, sammenhæng, omfang og formål. Det betyder, at graden af risikoen for den registreredes grundlæggende rettigheder eller frihedsrettigheder, herunder retten til privatliv, er bestemmende for, om en lejligheds-

vis behandling af særlige kategorier af personoplysninger efter forordningens artikel 9, stk. 1, eller oplysninger om straffedomme og lovovertrædelser efter artikel 10, i et ikke stort omfang, udløser en forpligtelse til at udpege en repræsentant efter artikel 27, stk. 1.

Offentlige myndigheder eller organer er efter forordningens artikel 27, stk. 2, litra b, ikke forpligtede til at udpege en repræsentant i EU.

Det følger endvidere af forordningens artikel 27, stk. 3, at repræsentanten skal være etableret i én af de EU-medlemsstater, hvor de registrerede, hvis personoplysninger behandles i forbindelse med udbuddet af varer eller tjenesteydelser eller hvis adfærd overvåges, er.

I henhold til artikel 27, stk. 4, skal navnlig tilsynsmyndigheden og den registrerede kunne rette henvendelse til repræsentanten – ud over eller i stedet for den dataansvarlige eller databehandleren – i forbindelse med alle sager vedrørende behandling af personoplysninger med henblik på at sikre overholdelse af forordningens bestemmelser.

Den dataansvarliges eller databehandlerens udpegning af en repræsentant berører efter artikel 27, stk. 5, i lighed med gældende ret, ikke eventuelle retslige skridt mod den dataansvarlige eller databehandleren selv, herunder erstatningsansvar i medfør af forordningen.

5.4.4. Overvejelser

Databeskyttelsesforordningens artikel 27 om repræsentanter indeholder som nævnt regler, der til en vis grad udvider og ændrer de krav, der stilles vedrørende repræsentanter efter gældende ret. Der vil således ikke ske en fuldstændig videreførelse af gældende ret for så vidt angår denne bestemmelse, når artikel 27 i medfør af forordningen skal anvendes i stedet for databeskyttelsesdirektivet og persondataloven fra den 25. maj 2018.

5.5. Databehandler, artikel 28

5.5.1. Præsentation

Formålet med en nærmere beskrivelse af databehandlerens forpligtelser i databeskyttelseslovgivningen er at skabe klarhed over databehandlerens rolle, og at denne alene kan behandle oplysninger på vegne af den dataansvarlige. Dermed kan databehandleren ikke selv definere, til hvilket formål og med hvilke midler, der skal ske behandling af personoplysninger.

Persondataloven indeholder i § 3, nr. 5, en definition af en databehandler. Dernæst følger en nærmere fastsættelse af dennes forpligtelser i lovens §§ 41 og 42. Endvidere indeholder

databeskyttelsesforordningen i artikel 4, nr. 8, en lignende definition af en databehandler. I forordningen er der desuden i artikel 28 en specifik bestemmelse om databehandleren og dennes forpligtelser efter forordningen.

5.5.2. Gældende ret

Det følger af persondatalovens § 3, nr. 5, at en databehandler er den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.

Bestemmelsen er baseret på databeskyttelsesdirektivets artikel 2, litra e. I direktivet anvendes begrebet "registerfører" i stedet for en databehandler. Det følger imidlertid af bemærkningerne til persondataloven, at der ikke er tilsigtet en indholdsmæssig ændring i den danske implementering af direktivet i forhold til direktivets definitioner, herunder definitionen af en databehandler.[526]

Det centrale ved definitionen af en databehandler er, at denne behandler oplysninger på den dataansvarliges vegne. Det betyder, at en databehandler ikke behandler oplysninger på egne vegne. Dermed har en databehandler efter gældende ret ikke ret til at bestemme over formålet og de hjælpemidler, den pågældende behandling af personoplysninger skal ske efter og har ej heller ret til at f.eks. slette eller videregive oplysninger uden instruks fra den dataansvarlige. En databehandler handler således alene efter instruks fra den dataansvarlige og må derfor kun anvende de pågældende oplysninger til udførslen af den konkrete opgave for den dataansvarlige.

En databehandler kan være såvel en privat virksomhed som en offentlig myndighed f.eks. en kommune, der kan agere som databehandler på vegne af én eller flere myndigheder.

Der kan ifølge Artikel 29-gruppens udtalelse om henholdsvis "registerfører" og "registeransvarlig" opstilles to grundlæggende betingelser for, om der er tale om en databehandler.[527] Der skal for det første være tale om en retlig selvstændig enhed i forhold til den dataansvarlige. Det betyder, at der f.eks. ikke er tale om en databehandler, når en virksomhed, der er dataansvarlig for en behandling, overlader denne til en anden afdeling inden for samme virksomhed. Dernæst er det et krav, at den pågældende behandler oplysninger på

[526] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 3, nr. 5.
[527] Artikel 29-gruppen: Artikel 29-gruppens udtalelse nr. 1/2010 om begreberne "registeransvarlig" og "registerfører", (WP 169), s. 25.

den dataansvarliges vegne. Et eksempel herpå kan være en virksomhed, der leverer en hosting-ydelse på internettet[528] eller en cloud-leverandør.[529]

5.5.2.1. Behandlingssikkerhed

Persondataloven indeholder to bestemmelser, der specifikt omhandler databehandleren, og som definerer dennes forpligtelser med hensyn til instruks og sikkerhed.[530]

Det følger således af persondatalovens § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov. Bestemmelsen er baseret på direktivets artikel 16, som har et lignende indhold.

Det fremgår af lovens § 41, stk. 1, at kravet om alene at handle efter instruks gælder for databehandleren selv samt enhver, der udfører arbejde under denne, og som får adgang til personoplysninger.

Der stilles efter bestemmelsen ikke særlige formkrav til den dataansvarliges instruks. Det må således lægges til grund, at en instruks både kan følge af en bestemt stilling eller ved, at den dataansvarlige autoriserer en ansat eller andre til at have adgang til bestemte oplysninger.[531]

Kravet om instruks indebærer, at den pågældende person ikke må behandle oplysninger til andre end de formål, som den dataansvarlige har fastsat. Ligeledes må den pågældende person ikke behandle oplysninger efter instruks fra andre end den dataansvarlige.

Forpligtelser med hensyn til behandlingssikkerhed følger af persondatalovens § 41, stk. 3. Det følger således af bestemmelsens 1. pkt., at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

[528] Artikel 29-gruppen: Artikel 29-gruppens udtalelse nr. 1/2010 om begreberne "registeransvarlig" og "registerfører", (WP 169), s. 25.
[529] Datatilsynets j.nr. 2011-082-0216. (Microsoft udtalelse).
[530] Artikel 29-gruppen: Artikel 29-gruppens udtalelse nr. 1/2010 om begreberne "registeransvarlig" og "registerfører", (WP 169), s. 26.
[531] Persondataloven med kommentarer (2015), s. 546.

Det følger endvidere af lovens § 41, stk. 3, 2. pkt., at tilsvarende gælder for databehandlere. Der er således tale om en selvstændig pligt for databehandlere til at efterleve de overordnede krav til behandlingssikkerheden.

Der er tale om en selvstændig forpligtelse for databehandleren, idet denne forpligtelse eksisterer uanset, hvordan forholdet mellem den dataansvarlige og databehandleren ellers er reguleret. Det vil sige, at kravet om, at databehandleren skal iværksætte den fornødne behandlingssikkerhed, ikke blot er en forpligtelse, som følger af den databehandleraftale, der efter lovens § 42 skal være indgået mellem den dataansvarlige og databehandler.

Endvidere følger det af lovens § 42, stk. 2, at de sikkerhedsbestemmelser, der er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne.[532] Dermed er en databehandler, der udøver sin virksomhed i Danmark, omfattet af de danske regler om behandlingssikkerhed i persondatalovens § 41, uanset om denne udfører arbejde på vegne af en dataansvarlig, der er etableret i Danmark eller i et andet land.

Hvis databehandleren er etableret i et andet EU-land, gælder de regler om sikkerhedsforanstaltninger, som er fastsat i det pågældende lands databeskyttelseslovgivning.[533]

Danske dataansvarlige, som er en offentlig myndighed, skal desuden iagttage reglerne i sikkerhedsbekendtgørelsen, uanset om behandlingen udføres af en databehandler, der er etableret i en anden medlemsstat.

Det bemærkes, at sikkerhedsbekendtgørelsens § 7, indeholder et krav om, at hvis en behandling foretages af en databehandler, skal der foreligge en skriftlig aftale med den dataansvarlige, hvoraf det fremgår, at reglerne i sikkerhedsbekendtgørelsen ligeledes gælder for behandlingen ved databehandleren. Det betyder, at hvis en behandling på vegne af en dansk offentlig myndighed finder sted hos en databehandler, der er etableret i et andet EU-land, skal databehandlerens behandling alligevel ske efter reglerne i sikkerhedsbekendtgørelsen.

Det skal desuden bemærkes, at persondatalovens § 41, stk. 3, er baseret på artikel 17, stk. 1, i databeskyttelsesdirektivet. Det følger af direktivets artikel 17, stk. 1, at medlemsstaterne fastsætter bestemmelser om, at den dataansvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et

[532] Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 327-328.
[533] Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 328.

net, samt mod enhver anden form for ulovlig behandling. Herudover følger det af artikel 17, stk. 1, 2. afsnit, at disse foranstaltninger, under hensyn til det aktuelle niveau og omkostningerne forbundet med deres iværksættelse, skal tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes.

Det følger af ordlyden af direktivets artikel 17, stk. 1, at det alene er den dataansvarlige, der er underlagt denne forpligtelse, hvorimod det efter persondatalovens § 41, stk. 3, både er den dataansvarlige og databehandleren, der er forpligtede hertil.

Dog skal det bemærkes, at det fremgår af direktivets artikel 17, stk. 2, at såfremt den dataansvarlige antager en databehandler, skal denne vælge en behandler, som kan sikre den nødvendige garanti med hensyn til tekniske og organisatoriske foranstaltninger. Samtidig skal den dataansvarlige vælge en databehandler, som også kan påse, at disse foranstaltninger overholdes. Herudover er der efter artikel 17, stk. 3, pligt til, at der foreligger en kontrakt mellem den dataansvarlige og databehandleren, hvoraf det skal fremgå, at forpligtelserne til at iværksætte de nødvendige foranstaltninger, såsom behandlingssikkerheden, ligeledes påhviler databehandleren. Dermed skal databehandleren, til trods for at denne ikke eksplicit er nævnt som pligtsubjekt i artikel 17, stk. 1, fortsat efter direktivet, iværksætte de fornødne sikkerhedsforanstaltninger, når denne behandler personoplysninger omfattet af direktivet.[534] Dermed kan det umiddelbart lægges til grund, at databehandleren, til trods for, at denne ikke er angivet som pligtsubjekt efter artikel 17 i databeskyttelsesdirektivet, efter artikel 17, stk. 2 og 3, i praksis skal overholde de samme forpligtelser som den dataansvarlige skal efter artikel 17, stk. 1. På baggrund heraf er der, til trods for forskellene i ordlyden, ikke materiel forskel mellem artikel 17, stk. 1, og dennes implementering i dansk ret i persondatalovens § 41, stk. 3.

I persondatalovens § 42 opstilles forskellige krav til en dataansvarlig, som overlader en behandling af oplysninger til en databehandler. Det følger af bestemmelsen, at når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.

5.5.2.2. Databehandleraftale

Herudover følger det af persondatalovens § 42, stk. 2, at hvis den dataansvarlige benytter sig af en databehandler, skal der indgås en skriftlig aftale herom med databehandleren. Bestemmelsen har sin baggrund i databeskyttelsesdirektivets artikel 17, stk. 3 og 4.

[534] Artikel 29-gruppen: Artikel 29-gruppens udtalelse nr. 1/2010 om begreberne "registeransvarlig" og "registerfører", (WP 169), s. 26.

Det følger af § 42, stk. 2, og direktivets artikel 17, stk. 3 og 4, at i enhver situation, hvor en dataansvarlig overlader en behandling til en databehandler, skal der være en skriftlig aftale herom. Det følger endvidere af bestemmelsen, at det skal fremgå af aftalen, at databehandleren alene handler efter instruks fra den dataansvarlige, som reguleret ved persondatalovens § 41, stk. 1. Herudover skal det fremgå af aftalen, at reglerne i persondatalovens § 41, stk. 3-5, ligeledes gælder for databehandlingen ved databehandleren. Hvis databehandleren er etableret i en anden medlemsstat, skal det desuden fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne.

Hvordan en databehandleraftale konkret udformes beror, ud over de specifikke krav hertil i bestemmelsen, på en konkret vurdering af, om der er behov for at indgå en mere detaljeret aftale for, at den dataansvarlige kan sikre sig, at forpligtelsen til at beskytte de pågældende personoplysninger også bliver efterlevet hos databehandleren.

Endvidere følger det af sikkerhedsbekendtgørelsen[535], at hvis den dataansvarlige er en offentlig myndighed, skal det fremgå af den skriftlige aftale med databehandleren, at reglerne i bekendtgørelsen ligeledes gælder for den behandling, som foretages af databehandleren.

Hverken direktivet eller persondataloven har eksplicitte bestemmelser for situationer, hvor den dataansvarlige overlader en behandling af oplysninger til flere databehandlere på én gang. Det kan imidlertid lægges til grund, at kravene til databehandlere også gælder, når en behandling af oplysninger er overladt til flere databehandlere på én gang. Der er således – hverken i direktivet eller persondataloven – noget til hinder for, at en dataansvarlig overlader en behandling af oplysninger til flere databehandlere på én gang.[536] Dette gælder både for så vidt angår flere databehandlere, samt når en databehandler overlader dele af behandlingsaktiviteterne til en underdatabehandler.

Disse underdatabehandlere skal imidlertid efterleve kravene i persondatalovens §§ 41 og 42, herunder følge de instrukser, som den dataansvarlige giver dem under behandlingen. Artikel 29-gruppen anbefaler i deres udtalelse om begreberne "registeransvarlig" og "registerfører", at man som dataansvarlig bør undgå en kæde af databehandlere og underdatabehandlere, idet dette kan forringe eller endda hindre en effektiv kontrol, medmindre ansvaret hos de forskellige parter i kæden er klart fastlagt. Herudover anfører Artikel 29-gruppen, at det er nødvendigt, at den dataansvarlige i sådanne tilfælde informeres om hovedelementer-

[535] Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, i medfør af § 41, stk. 5, i lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.
[536] Artikel 29-gruppens udtalelse om 1/2010 om begreberne "registeransvarlig" og "registerfører", (WP 169), s. 27.

ne i behandlingsstrukturen, det vil sige bl.a. om sikkerhedsforanstaltninger samt garantier for behandling i tredjeland. På den måde vil den dataansvarlige, ifølge Artikel 29-gruppen, stadig være i stand til at have kontrol med de oplysninger, som behandles på dennes vegne.[537]

5.5.3. Databeskyttelsesforordningen

I databeskyttelsesforordningens artikel 4, nr. 8, defineres en databehandler som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne. Forordningens definition af en databehandler svarer således til definitionen, der følger af persondatalovens § 3, nr. 5.

Forordningens artikel 28 indeholder specifikke regler om databehandleren og dennes forpligtelser. Det følger således af artikel 28, stk. 1, at hvis en behandling skal foretages på vegne af en dataansvarlig, benytter den dataansvarlige udelukkende databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandling opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder.

Hertil fremgår det bl.a. af præambelbetragtning nr. 81, at den dataansvarlige udelukkende bør benytte sig af databehandlere, der giver tilstrækkelige garantier, navnlig i form af ekspertise, pålidelighed og ressourcer, for implementering af tekniske og organisatoriske foranstaltninger, der opfylder kravene i forordningen.

5.5.3.1. Flere databehandlere

Som en nyskabelse i forhold til gældende ret, stilles der i artikel 28, stk. 2, betingelser for, hvornår en databehandler må benytte sig af andre databehandlere (underdatabehandlere). Det følger således af artikel 28, stk. 2, at databehandleren ikke må gøre brug af en underdatabehandler uden forudgående specifik eller generel skriftligt godkendelse fra den dataansvarlige. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

Dernæst følger det af artikel 28, stk. 4, at databehandleren skal opfylde yderligere betingelser end dem angivet i artikel 28, stk. 2, førend, at denne kan gøre brug af en underdatabehandler. Det følger således af artikel 28, stk. 4, at hvis en databehandler gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne

[537] Artikel 29-gruppens udtalelse nr. 1/2010 om begreberne "registeransvarlig" og "registerfører", (WP 169), s. 28.

af den dataansvarlige, pålægges denne underdatabehandler de samme databeskyttelsesforpligtelser som dem, der er fastsat i kontrakten eller et andet retligt dokument mellem den dataansvarlige og databehandleren som omhandlet i stk. 3, gennem en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret. I denne kontrakt eller det retlige dokument skal der navnlig være stillet de fornødne garantier for, at parterne vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren dermed fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

Det må på baggrund af artikel 28, stk. 2, lægges til grund, at databehandleren enten indhenter en generel godkendelse til at udlicitere en databehandling til en underdatabehandler, eller en specifik godkendelse hertil fra den dataansvarlige. Dermed har den dataansvarlige mulighed for at gøre indsigelse med en databehandlers brug af en underdatabehandler i den konkrete behandling af personoplysninger.

Dette er endvidere i overensstemmelse med de betingelser, der følger af Kommissionens afgørelse af 5. februar 2010 om standardkontraktbestemmelser for videregivelse af personoplysninger til databehandlere etableret i tredjelande i henhold til databeskyttelsesdirektivet, som omhandler tredjelandsoverførsel fra en dataansvarlig til en databehandler. Det følger således af standardbestemmelse 11 i bilaget til standardkontraktbestemmelserne, at dataimportøren (databehandleren) ikke overlader noget af den databehandling, han foretager på dataeksportørens (den dataansvarlige) vegne i henhold til standardbestemmelserne, uden den dataansvarliges forudgående skriftlige samtykke.

Herudover følger det af standardbestemmelse 11, at når databehandleren med den dataansvarliges samtykke, overlader sine forpligtelser i henhold til standardbestemmelserne, sker dette udelukkende ved indgåelse af en skriftlig aftale med underdatabehandleren, som herved pålægges de samme forpligtelser, som dem, der påhviler databehandleren i henhold til standardbestemmelserne. Dernæst følger det af bestemmelsen, at hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser i henhold til en sådan skriftlig aftale, er databehandleren fuldt ansvarlig over for den dataansvarlige for, at underdatabehandlerens forpligtelser i henhold til en sådan aftale opfyldes.

På baggrund af standardkontraktbestemmelserne, skal der således indgås en kontrakt mellem databehandleren og underdatabehandleren, såfremt databehandleren vælger at overlade dele af sin behandlingsaktivitet til en underdatabehandler.

Dette taler for, at det kan lægges til grund, at artikel 28, stk. 4, skal forstås således, at kravet om, at der skal indgås en kontrakt eller et andet retligt dokument, omhandler det retlige forhold mellem databehandleren og de eventuelle underdatabehandlere, denne gør brug af. Dermed stilles der i artikel 28, stk. 4, *ikke* krav om, at det er den dataansvarlige, der skal indgå særskilte aftaler med eventuelle underdatabehandlere. Den dataansvarlige kan i stedet blot holde sig til den databehandleraftale, der på baggrund af artikel 28, stk. 3, er indgået med databehandleren, og herefter give konkret eller generel tilladelse til, at databehandleren overlader behandlingen til underdatabehandlere. I stedet er det derfor databehandleren, der i medfør af artikel 28, stk. 4, skal indgå en kontrakt eller et andet retligt dokument i medfør af national eller EU-retten, med de underdatabehandlere, denne måtte vælge af gøre brug af.

I forhold til den konkrete ansvarsfordeling mellem databehandleren og dennes underdatabehandler, følger det eksplicit af artikel 28, stk. 4, at databehandleren er fuldt ud ansvarlig, såfremt en underdatabehandler ikke opfylder sine forpligtelser i medfør af bestemmelsen. Dermed hæfter en databehandler altid for en underdatabehandlers manglende efterlevelse af forordningens forskrifter.

Situationen er imidlertid anderledes, såfremt den dataansvarlige vælger at overlade en behandling af personoplysninger til to forskellige databehandlere. En sådan situation vil ikke være omfattet af artikel 28, stk. 2 og 4, idet der ikke er tale om, at en databehandler *gør brug* af en underdatabehandler til behandlingen. I stedet vil situationen være omfattet af artikel 28, stk. 3, hvorefter den dataansvarlige skal udarbejde en databehandleraftale med *hver* af de to databehandlere.

Det følger af artikel 28, stk. 5, at en databehandlers overholdelse af en godkendt adfærdskodeks, som omhandlet i artikel 40, eller en godkendt certificeringsmekanisme, som omhandlet i artikel 42, kan bruges som et element til at påvise fornødne garantier, som omhandlet i nærværende artikels stk. 1 og 4.

I forlængelse af artikel 28, stk. 3 og 4, følger det af artikel 28, stk. 6, at uden, at det berører en individuel kontrakt mellem den dataansvarlige og databehandleren, kan kontrakten eller det andet retlige dokument, der er omhandlet i artikel 28, stk. 3 og 4, helt eller delvis baseres på de standardkontraktbestemmelser, der er anført i artikel 28, stk. 7 og 8, herunder når de indgår i en certificering, der er meddelt den dataansvarlige eller databehandleren i henhold til artikel 42 og 43. Dermed kan den dataansvarlige og databehandleren anvende standardkontraktbestemmelser, som er fastsat af Kommissionen i medfør af artikel 28, stk. 7 og 8, til de kontrakter, der indgås med den dataansvarlige i henhold til bestemmelsens stk. 3 og 4.

For så vidt angår standardkontraktbestemmelser, følger det af artikel 28, stk. 7, at Kommissionen kan fastsætte sådanne bestemmelser i de tilfælde, der er omhandlet i artikel 28, stk. 3 og 4, og i overensstemmelse med undersøgelsesproceduren, der er omhandlet i artikel 93, stk. 2.[538]

Herudover kan en tilsynsmyndighed i medfør af artikel 28, stk. 8, ligeledes vedtage standardkontraktbestemmelser i de tilfælde, der er omhandlet i artikel 28, stk. 3 og 4, og i overensstemmelse med sammenhængsmekanismen, der er omhandlet i artikel 63.

For så vidt angår formkrav til kontrakten eller det andet retlige dokument, der er omhandlet i bestemmelsens stk. 3 og 4, skal disse i medfør af artikel 28, stk. 9, foreligge skriftligt, herunder elektronisk.

Endelig følger det af artikel 28, stk. 10, at hvis en databehandler overtræder forordningen ved at fastlægge formålene med og hjælpemidlerne til behandling, anses databehandleren for at være en dataansvarlig for så vidt angår den pågældende behandling, uden at dette berører artikel 82, 83 og 84. Konsekvensen heraf vil være, at denne "nye" dataansvarlige selvstændigt skal efterleve forordningens krav, herunder tilvejebringe et behandlingsgrundlag. I tilfælde, hvor en databehandler er overgået til at være en dataansvarlig, og denne ikke har behandlingshjemmel i databeskyttelsesforordningen, vil dette udgøre en overtrædelse af forordningen.

5.5.3.2. Databehandleraftale

I overensstemmelse med artikel 17, stk. 3, i direktivet og persondatalovens § 42, stk. 2, er den dataansvarlige ligeledes forpligtet til at indgå en aftale med databehandleren i medfør af forordningens artikel 28, stk. 3.

Det følger endvidere af præambelbetragtning nr. 79, at beskyttelse af registreredes rettigheder og frihedsrettigheder samt de dataansvarliges og databehandlernes ansvar, herunder erstatningsansvar, også i forbindelse med tilsynsmyndighedernes kontrol og foranstaltninger kræver en klar fordeling af ansvarsområderne i medfør af denne forordning, herunder når en dataansvarlig fastlægger formålene med og hjælpemidlerne til behandling sammen med andre dataansvarlige, eller når en behandlingsaktivitet foretages på vegne af en dataansvarlig. Dermed forudsætter en effektiv beskyttelse af bl.a. de registrerede personers rettigheder, at der er en klar fordeling af ansvarsområderne for så vidt angår dataansvarlige og databehandlernes ansvar, herunder når en dataansvarlig vælger at overdrage visse dele af behandlingsaktiviteterne til en databehandler.

[538] Det bemærkes, at det retligt er korrekt at henvise til artikel 92 om udøvelse af de delegerede beføjelser i stedet for artikel 93 om udvalgsprocedure.

Det følger herudover af artikel 28, stk. 3, at en databehandlers behandling skal være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige, og der fastsætter genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder.

De specifikke krav, der stilles til en databehandleraftale, følger af artikel 28, stk. 3, litra a til h. I forhold til gældende ret, stilles der i forordningen flere og mere detaljerede krav til selve databehandleraftalen.

For det første skal aftalen i medfør af artikel 28, stk. 3, litra a, fastsætte, at databehandleren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. I så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

Kravet om, at det af databehandleraftalen skal fremgå, at databehandleren alene må handle efter instruks følger ligeledes af gældende ret. Til forskel fra gældende ret, følger det imidlertid af forordningen, at det skal fremgå af databehandleraftalen, at instruksen fra den dataansvarlige efter forordningen skal være dokumenteret. Det uddybes ikke nærmere i bestemmelsen, hvorledes instruksen fra databehandleren skal dokumenteres. Men det må antages, at kravet betyder, at såvel den dataansvarlige som databehandleren skal dokumentere instruksen, så begge parter kan sikre sig, at forordningens regler er efterlevet i den konkrete behandling af personoplysninger.

Dernæst følger det af artikel 28, stk. 3, litra b, at det i aftalen endvidere skal fastsættes, at databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt. Det er en ny forpligtelse for databehandleren, at denne nu skal sikre sig, at personer som arbejder under databehandleren, er underlagt en fortrolighedsforpligtelse eller en passende lovbestemt tavshedspligt. Det må antages, at denne forpligtelse er opfyldt for offentlige myndigheder, der fungerer som databehandlere, idet offentlige ansatte er underlagt tavshedspligt, jf. forvaltningslovens § 27, stk. 1, jf. straffelovens § 152 og 152 c-f.

I overensstemmelse med gældende ret i direktivets artikel 17, stk. 2, og persondatalovens § 42, stk. 2, skal det desuden i medfør af forordningens artikel 28, stk. 3, litra c, fastsættes i

databehandleraftalen, at databehandleren iværksætter alle foranstaltninger, som kræves i henhold til artikel 32 om behandlingssikkerhed.

Som endnu en nyskabelse i forhold til gældende ret, skal det i medfør af bestemmelsens litra d, fremgå af databehandleraftalen, at databehandleren opfylder de betingelser, der er omhandlet i stk. 2 og 4, for at gøre brug af en underdatabehandler.

Herudover følger det af bestemmelsens litra e, at det skal fremgå af databehandleraftalen, at databehandleren under hensyntagen til behandlingens karakter så vidt muligt bistår den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III. Der er tale om en ny forpligtelse for databehandleren, idet denne efter gældende ret ikke er underlagt denne forpligtelse.

Ud over at bistå den dataansvarlige med dennes forpligtelse over for de registrerede personer, skal databehandleren som følge af litra f, endvidere bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren. Databehandleren er allerede selv forpligtet til at efterleve sine forpligtelser efter artikel 32 om behandlingssikkerhed, som følge af kravet til databehandleraftalen i artikel 28, stk. 3, litra c, og som følge af ordlyden af artikel 32, stk. 1. Denne forpligtelse udvides således, så databehandleren skal bistå den dataansvarlige med behandlingssikkerhed efter artikel 32, men også med at anmelde brud på persondatasikkerheden til tilsynsmyndigheden efter artikel 33 og endelig med at foretage underretning om brud på persondatasikkerheden i forhold til de registrerede i medfør af artikel 34. Dernæst skal databehandleren endvidere bistå den dataansvarlige med sin forpligtelse til at udarbejde konsekvensanalyser vedrørende databeskyttelse i medfør af artikel 35 samt foretage forudgående høring af tilsynsmyndigheden, såfremt en konsekvensanalyse viser, at den pågældende behandling vil føre til høj risiko i medfør af artikel 36.

Herudover stilles der i artikel 28, stk. 3, litra g, krav om, at det skal fremgå af databehandleraftalen, om denne enten skal slette eller tilbagelevere alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og sletter eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne. Det er den dataansvarlige, der træffer valget om, hvorvidt databehandleren skal foretage en sletning eller tilbagelevering af de pågældende oplysninger.

Endelig skal det i medfør af bestemmelsens litra h fremgå af databehandleraftalen, at databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af krave-

ne i artikel 28, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

Allerede fordi der ikke stilles krav om, at den dataansvarlige skal have en bestemt stillingsbetegnelse, såsom revisor, må det betyde, at der med "en anden revisor" *ikke* henvises til en stillingsbetegnelse i artikel 28, stk. 3, litra h.

For så vidt angår første afsnit, litra h, underretter databehandleren omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Ovenstående foranstaltninger skal således til enhver tid fremgå af en databehandleraftale, når en dataansvarlig vælger at overlade behandlingen af personoplysninger til en databehandler. Det følger endvidere af artikel 28, stk. 9, at selve kontrakten eller det andet retlige dokument, som udgør en databehandleraftale i medfør af artikel 28, stk. 3, skal foreligge skriftligt, herunder elektronisk. Der er tale om et nyt formkrav i forhold til gældende ret, idet databehandleraftalen nu også skal foreligge elektronisk.

5.5.4. Overvejelser

Artikel 28 i databeskyttelsesforordningen om databehandleren indeholder nye forpligtelser for databehandleren i forhold til gældende ret. Nyskabelsen består for det første i, at der efter artikel 28, stk. 3, stilles flere og mere detaljerede krav til indholdet i en databehandleraftale, og dermed til databehandlerens forpligtelser over for den dataansvarlige, end efter gældende ret. Disse krav vil imidlertid kunne blive iagttaget ved at benytte standardkontraktbestemmelser som anført i artikel 28, stk. 7 og 8.

Dernæst er det en nyskabelse, at artikel 28 indeholder eksplicitte betingelser for, hvornår en databehandler må benytte sig af underdatabehandlere, samt hvorledes dette forhold reguleres. Det følger heraf, at såfremt en databehandler vælger at benytte sig af en underdatabehandler til en specifik behandlingsaktivitet, skal denne underdatabehandler indgå en ny kontrakt eller et andet retligt dokument med databehandleren, der afspejler den aftale, som databehandleren har med den dataansvarlige, samt at denne aftale fastsætter passende tekniske og organisatoriske foranstaltninger for behandlingen af personoplysninger.

5.6. Instruks, artikel 29

5.6.1 Præsentation

Databeskyttelsesdirektivets artikel 16 og persondatalovens § 41, stk. 1, omhandler et krav om instruks. Dette krav videreføres i databeskyttelsesforordningens artikel 29.

5.6.2 Gældende ret

Behandling, der udføres for den dataansvarlige og databehandleren, er reguleret i henholdsvis databeskyttelsesdirektivets artikel 16 og persondatalovens § 41, stk. 1.

Det følger således af direktivets artikel 16, at enhver, der udfører arbejde under den dataansvarlige eller databehandleren, herunder databehandleren selv, og som får adgang til personoplysninger, kun må behandle disse efter instruks fra den dataansvarlige, bortset fra tilfælde, der er fastsat i lovgivningen.

Det følger ligeledes af persondatalovens § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Det fremgår af lovens § 41, stk. 1, at kravet om alene at handle efter instruks gælder for databehandleren selv samt enhver, der udfører arbejde under denne, og som får adgang til personoplysninger. Dermed må vedkommende ikke anvende oplysningerne til andre formål end til brug for løsning af netop den opgave, som denne er blevet pålagt af den dataansvarlige. Det betyder f.eks., at en databehandler ikke må videregive oplysninger til tredjemand uden instruks herom i medfør af § 41, stk. 1, fra den dataansvarlige.[539]

Det betyder endvidere, at vedkommende ikke må behandle oplysninger efter instruks fra andre end den dataansvarlige, medmindre dette følger af lovgivningen.

Der stilles efter bestemmelsen ikke særlige formkrav til den dataansvarliges instruks. Det må således lægges til grund, at en instruks både kan følge af en bestemt stilling eller af, at den dataansvarlige autoriserer en ansat eller andre til at have adgang til bestemte oplysninger.[540]

[539] Persondataloven med kommentarer (2015), s. 547.
[540] Persondataloven med kommentarer (2015), s. 546.

5.6.3 Databeskyttelsesforordningen

Behandling, der udføres for den dataansvarlige og databehandleren, er reguleret i forordningens artikel 29.

Det følger således af forordningens artikel 29, at databehandleren og enhver, der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, kun behandler disse oplysninger efter instruks fra den dataansvarlige, medmindre andet kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

Kravet om alene at handle efter instruks i forordningen svarer til det krav, der følger af direktivets artikel 16 og persondatalovens § 41, stk. 1. Det må derfor antages, at kravet om instruks efter forordningen ligeledes gælder for databehandleren selv samt enhver, der udfører arbejde under denne og
får adgang til personoplysninger.

Dernæst stilles der ikke særlige formkrav til selve instruksen i forordningens artikel 29. Det må imidlertid i overensstemmelse med gældende ret antages, at en instruks både kan følge af en bestemt stilling eller af, at den dataansvarlige autoriserer en ansat eller andre til at have adgang til bestemte oplysninger.

5.6.4 Overvejelser

Databeskyttelsesforordningens artikel 29 om behandling, der udføres for den dataansvarlige eller databehandleren, svarer til det krav om instruks, der følger af gældende ret i databeskyttelsesdirektivets artikel 16 og persondatalovens § 41, stk. 1. Forordningens artikel 29 er således en videreførelse af gældende ret.

5.7. Fortegnelser over behandlingsaktiviteter, artikel 30, stk. 1-4

5.7.1. Præsentation

Det følger af anmeldelsespligten i direktivets artikel 18, stk. 1, og persondatalovens §§ 43, stk. 1 og 48, at der i visse situationer skal ske anmeldelse til Datatilsynet, og at denne anmeldelse skal indeholde en optegnelse over de behandlingsaktiviteter, der anmeldes.

Databeskyttelsesforordningen lægger op til en anden ordning. Det følger således af forordningens artikel 30, at den dataansvarlige og databehandleren i visse tilfælde skal føre *interne* fortegnelser over deres behandling af personoplysninger. Dette ligger fint i tråd med forordningens risikobaserede tilgang og fokus på ansvarlighed (”accountability”).

5.7.2. Gældende ret

5.7.2.1. Anmeldelsesordningen

Persondatalovens kapitel 12-14 indeholder regler om anmeldelse af behandling af personoplysninger til tilsynsmyndigheden mv. Bestemmelserne i persondataloven er baseret på artikel 18-21 i databeskyttelsesdirektivet.

Persondatalovens kapitel 12 (§§ 43-47) regulerer således anmeldelse af behandling, der udføres for *offentlige* dataansvarlige. Offentlige dataansvarlige skal i visse tilfælde, forud for behandlingen af personoplysninger, foretage anmeldelse til Datatilsynet samt indhente tilsynets udtalelse.

Persondatalovens kapitel 13 (§§ 48-51) regulerer anmeldelse af behandling af personoplysninger, der udføres af *private* dataansvarlige. Private dataansvarlige skal i visse tilfælde, forud for behandlingen af personoplysninger, foretage anmeldelse af en behandling af personoplysninger til Datatilsynet samt indhente tilsynets tilladelse til behandlingen.

5.7.2.2. Anmeldelsens indhold

De indholdsmæssige krav til en anmeldelse til tilsynsmyndigheden for behandling foretaget af en *offentlig myndighed* følger af persondatalovens § 43, stk. 2. Bestemmelsen er baseret på direktivets artikel 19, som fastsætter, hvilke oplysninger en anmeldelse til tilsynsmyndighederne som minimum skal indeholde. Medlemsstaterne kan endvidere på baggrund af artikel 19 præcisere, hvilke oplysninger en anmeldelse herudover skal indeholde. På baggrund heraf er der i persondatalovens § 43, stk. 2, opstillet de i artikel 19 nævnte krav samt yderligere præciserende krav til indholdet i en anmeldelse af behandling af oplysninger til Datatilsynet.

Det følger af persondatalovens § 48, stk. 2, at anmeldelse af behandling, som foretages på vegne af en *privat dataansvarlig*, skal indeholde de oplysninger, som fremgår af § 43, stk. 2. Der gælder således de samme indholdsmæssige krav til anmeldelser for henholdsvis private såvel som offentlige myndigheder.

Udfyldelsen af en anmeldelse giver den dataansvarlige anledning til at beskrive en eller en række behandlinger og således overveje behandlingens rimelighed samt nødvendigheden.

Det skal imidlertid bemærkes, at den dataansvarlige i medfør af de grundlæggende principper for behandling af oplysninger i persondatalovens § 5, som altid skal iagttages ved behandling af oplysninger, til enhver tid er forpligtet til at overveje en behandlings rimelighed samt nødvendigheden heraf. Denne vurdering skal en dataansvarlig foretage løben-

de ved enhver behandling af oplysninger, og ikke blot når denne foretager anmeldelse af behandlingen til Datatilsynet.

Endvidere er det den dataansvarlige, der i medfør af persondatalovens regler, har ansvaret for en behandling af personoplysninger, og det er dermed også denne, der skal kunne påvise over for henholdsvis de registrerede personer samt tilsynsmyndigheden, at den pågældende behandling sker i overensstemmelse med persondatalovens regler.

Under alle omstændigheder er udfyldelsen af en anmeldelse af ens behandlingsaktivitet til tilsynet en god anledning til at foretage de overvejelser, en dataansvarlig til enhver tid skal foretage, når der sker behandling af oplysninger omfattet af persondataloven.

Det følger af ordlyden af direktivets artikel 18, stk. 1, at genstanden for en anmeldelse er en behandling eller en række behandlinger, hvis formål er identiske eller indbyrdes relaterede. Det er således ikke edb-systemer eller systemgange, der er genstand for anmeldelsen, men selve behandlingen af personoplysninger. På baggrund heraf må det antages, at der ikke skal foretages en selvstændig anmeldelse af hver enkelt behandling, såsom hver enkelt videregivelse, indsamling mv., som den dataansvarlige foretager.[541] Det betyder samtidig, at det ikke er nødvendigt at anmelde hver enkelt konkret behandling helt ned på individniveau, f.eks. hver enkelt indsamling af oplysninger om en bestemt person.

Det følger endvidere både af direktivets artikel 19, stk. 1, og persondatalovens § 43, stk. 2, nr. 2, at en anmeldelse skal indeholde en angivelse af behandlingens betegnelse og formål. Det fremgår af bemærkningerne til persondataloven og af Registerudvalgets betænkning nr. 1345, at angivelsen af formålet med behandlingen ifølge Registerudvalget må skulle forstås på den måde, at der skal kunne formuleres et samlet, logisk sammenhængende formål med en behandling eller en række af behandlinger, som anmeldes på én anmeldelse.[542] Det betyder, at flere behandlinger kan anmeldes på én gang, så længe disse formål er indbyrdes relaterede eller identiske.[543]

Det kan f.eks. være delformål, som har en indbyrdes sammenhæng, såsom hvis der er tale om den samme opgave eller lovgrundlag for behandlingerne mv.

Det betyder endvidere, at en anmeldelse kan dække behandlinger af personoplysninger, der foretages både manuelt og elektronisk og behandlinger, der fysisk foregår forskellige ste-

[541] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 343.
[542] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, i de specielle bemærkninger til § 43 og Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 343.
[543] Datatilsynets vejledning nr. 125 af den 10. juli 2010 om anmeldelse i henhold til kapitel 12 i lov om behandling af oplysninger (til offentlige myndigheder), afsnit 2.2.

der. Dernæst kan en anmeldelse også dække forskellige funktioner, som har samme overordnede formål, såsom journalisering, sagsbehandling, registrering af ind- og udbetalinger mv.[544]

Af konkrete krav til indholdet af anmeldelsen, følger det herudover af persondatalovens § 43, stk. 2, *nr. 1*, at anmeldelsen for det første skal indeholde navn og adresse på den dataansvarlige, dennes eventuelle repræsentant og på en eventuelt databehandler.

Herudover skal anmeldelsen efter § 43, stk. 2, *nr. 2*, indeholde en angivelse af formålet og en betegnelse af behandlingen. Det må lægges til grund, at formålet i anmeldelsen skal angives i overensstemmelse med Registerudvalgets bemærkninger herom, således at der formuleres et samlet, logisk sammenhængende formål med den række af behandlinger, der anmeldes. Selve behandlingens betegnelse vil ofte være en angivelse af det sammenhængende formål med den række af behandlinger, som anmeldes.

Dette krav til anmeldelsen afspejler princippet om formålsbestemthed efter persondatalovens § 5, stk. 2, som altid skal iagttages ved behandling af personoplysninger. Dermed skal den dataansvarlige, allerede forud for at en behandling iværksættes, vurdere, til *hvilke udtrykkeligt angivne* og saglige formål behandlingen skal ske. Der er således alene efter § 43, stk. 2, nr. 2, tale om, at det formål, som alle dataansvarlige efter § 5, stk. 2, skal definere ved en behandling af personoplysninger, skal skrives ned i anmeldelsen til Datatilsynet.

Som eksempel på angivelse af flere behandlinger til opfyldelse af samme formål fra Datatilsynets fortegnelse over anmeldelser kan nævnes betegnelsen *personaleadministration*, som vil have til formål at behandle oplysninger om ansatte og ansøgere hos den dataansvarlige i forbindelse med ansættelse, arbejdsforløb og ophør af ansættelse.[545]

Det samme kan gøres gældende ved f.eks. en kommunes behandling af personoplysninger i forbindelse med beskæftigelse og kommunale ydelser, hvor der formentlig vil være flere forskellige delformål, såsom kommunal udbetaling af kommunale ydelser, råd og vejledning, kommunal indsats vedrørende jobformidling mv. I et sådant tilfælde vil disse delformål have et samlet, logisk sammenhængende formål, som vil kunne angives som en kommunes behandling af personoplysninger i forbindelse med dennes forpligtelser inden for beskæftigelse og kommunale ydelser, hvilket afspejles i fortegnelserne over kommuners fællesanmeldelser offentliggjort i Datatilsynets fortegnelse.

[544] Datatilsynets vejledning nr. 125 af den 10. juli 2010 om anmeldelse i henhold til kapitel 12 i lov om behandling af oplysninger (til offentlige myndigheder), afsnit 2.2.
[545] Se Datatilsynets fortegnelse på www.datatilsynet.dk.

Endvidere følger det af § 43, stk. 2, *nr. 3*, at en anmeldelse skal indeholde en generel beskrivelse af behandlingen af personoplysninger. Det følger af Registerudvalgets betænkning nr. 1345, at en sådan generel beskrivelse bør bestå af en opregning af de typer af behandlinger, som er omfattet af anmeldelsen, såsom f.eks. indsamling af oplysninger fra de registrerede eller bestemte myndigheder, anvendelse af oplysninger til bestemte delformål samt hvorvidt oplysningerne behandles elektronisk eller manuelt.[546]

Dermed skal den dataansvarlige allerede forud for, at en behandling iværksættes, kortlægge hvilke typer af behandlinger den konkrete behandling af oplysninger indebærer. Det skal bemærkes, at den dataansvarlige som følge af persondatalovens § 5, stk. 3, alene må behandle oplysninger, som er relevante og tilstrækkelige og ikke omfatter mere, end hvad der kræves til opfyldelse af formålet med behandlingen. En sådan vurdering af en behandling af personoplysninger forudsætter, at den dataansvarlige har overblik over, hvilke typer af behandlinger den konkrete behandling af personoplysninger indebærer. Der er således tale om et krav til den dataansvarlige, der også er afspejlet i persondatalovens § 5, stk. 3, når den dataansvarlige skal foretage en vurdering af, hvilke typer af behandlinger den konkrete behandling indebærer i medfør af § 43, stk. 2, nr. 3.

Denne beskrivelse efter lovens § 43, stk. 2, nr. 3, kan, ifølge Registerudvalget, være nødvendig for Datatilsynets vurdering af, om de enkelte behandlinger i den række af behandlinger, der anmeldes isoleret set er i overensstemmelse med lovgivningen. Herudover er beskrivelsen af, hvorvidt behandlingen sker manuelt eller elektronisk med til, at Datatilsynet kan vurdere sikkerhedsforanstaltningerne ved behandlingen.

Registerudvalget anførte endvidere i betænkning nr. 1345, at en generel beskrivelse af behandlingen giver borgerne mulighed for at få en langt mere fyldestgørende indsigt i, hvad den pågældende behandling går ud på, hvilket også bidrager til offentlighed omkring anmeldelser, som er et af formålene med anmeldelsesordningen.

Den generelle beskrivelse kan holdes på et overordnet plan, idet der blot skal angives tilstrækkelige oplysninger til, at Datatilsynet bliver i stand til at vurdere, om der skal foretages en nærmere vurdering af behandlingen af personoplysninger.

Dernæst følger det af persondatalovens § 43, stk. 2, *nr. 4*, at en anmeldelse til Datatilsynet skal indeholde en beskrivelse af kategorierne af registrerede og af de typer af oplysninger, der vedrører dem.

[546] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 344.

En beskrivelse af kategorierne af de registrerede personer må antages at udgøre en nærmere beskrivelse af, hvilke registrerede man konkret behandler oplysninger om. For en offentlig myndighed kan dette f.eks. være oplysninger om borgere og virksomheder, der har ansøgt om en ydelse. For private kan dette f.eks. være nuværende og tidligere medarbejdere ved anmeldelse af behandlingen af oplysninger i forbindelse med en personaleadministration.

Endvidere skal der være en beskrivelse af de typer af oplysninger, der behandles om de registrerede personer.

Dermed skal den dataansvarlig, allerede forud for behandlingen iværksættes, kortlægge, hvilke kategorier af registrerede, der er nødvendige at behandle oplysninger om, og hvilke typer oplysninger, der er relevant for den konkrete behandling af personoplysninger. Der er også her tale om et krav, der allerede er afspejlet i persondatalovens § 5, stk. 3, når den dataansvarlige skal foretage en vurdering af, hvilke kategorier af registrerede personer og de oplysninger, der skal behandles om disse.

Desuden skal der i fortegnelsen i medfør af persondatalovens § 43, stk. 2, *nr. 5*, medtages en beskrivelse af de modtagere eller kategorier af modtagere, som oplysningerne kan overføres til. Den dataansvarlige skal således kortlægge, hvorvidt der vil ske overførsel af oplysninger til en tredjemand, og hvem disse i givet fald er. Inden for det kommunale område kan dette f.eks. være videregivelse af oplysninger til SKAT, ATP, Feriekonto mv.

Det er alene de overførsler til tredjemænd eller andre modtagere, som må forudses at skulle ske på regelmæssig basis, som skal anføres i anmeldelsen.[547] Det betyder bl.a., at overførsler af oplysninger mellem myndigheder skal nævnes, såfremt de sker regelmæssigt.

Det følger af persondatalovens § 5, stk. 2, at en behandling af oplysninger skal tjene et sagligt formål. Dermed skal en videregivelse af personoplysninger til en tredjemand ligeledes altid tjene et sagligt formål for, at behandlingen er i overensstemmelse med persondatalovens regler. Dermed er der tale om et krav om, der allerede er afspejlet i persondatalovens § 5, stk. 2, at den dataansvarlige skal beskrive de påtænkte modtagere i en anmeldelse til Datatilsynet i medfør af i persondatalovens § 43, stk. 2, nr. 4.

Herudover følger det af persondatalovens § 43, stk. 2, nr. 6, at det skal fremgå af anmeldelsen, hvilke påtænkte overførsler til tredjelande den konkrete behandling vil indebære. Dermed skal den dataansvarlige have klarhed over, hvorvidt der vil ske overførsel af op-

[547] Datatilsynets vejledning nr. 125 af den 10. juli 2010 om anmeldelse i henhold til kapitel 12 i lov om behandling af oplysninger (til offentlige myndigheder), til pkt. 5.

lysninger til tredjelande og angive disse overførsler, herunder modtagere, i anmeldelsen til Datatilsynet.

Desuden skal anmeldelsen efter lovens § 43, stk. 2, *nr. 7*, indeholde en generel beskrivelse af de foranstaltninger, der iværksættes af hensyn til behandlingssikkerheden. Offentlige myndigheder er omfattet af Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen), der er udstedt i medfør af persondatalovens § 41, stk. 5. Det vil således skulle fremgå af anmeldelsen, om der træffes sikkerhedsforanstaltninger, som beskrevet i sikkerhedsbekendtgørelsen.

Det følger af persondatalovens § 41, stk. 3, 1. pkt., at den dataansvarlige har ansvaret for at sikre, at der træffes de nødvendige sikkerhedsforanstaltninger, når der behandles oplysninger omfattet af persondataloven. Dermed er det også op til den dataansvarlige at påvise over for de registrerede personer og tilsynsmyndigheden, at den dataansvarlige har sikret de nødvendige sikkerhedsforanstaltninger. Kravet til anmeldelsen i lovens § 43, stk. 2, nr. 7, er et krav om, at den vurdering, som den dataansvarlige til enhver tid ved behandling af oplysninger skal foretage, også skal beskrives til tilsynet i anmeldelsen af den påtænkte behandling.

Herudover skal tidspunktet for påbegyndelsen af behandlingen samt tidspunktet for sletning af oplysningerne som følge af persondatalovens § 43, stk. 2, nr. 8 og 9, fremgå af anmeldelsen. Det følger af persondatalovens § 5, stk. 5, at de indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Dermed skal den dataansvarlige til enhver tid vurdere, om det fastsatte saglige formål med behandlingen er opfyldt for at vurdere, om oplysningerne skal slettes. Der er således i lovens § 43, stk. 2, nr. 8 og 9, tale om overvejelser, som den dataansvarlige i forvejen efter § 5, stk. 5, skal foretage.

For så vidt angår ændringer i de i § 43, stk. 2, nævnte oplysninger, der allerede er anmeldt til Datatilsynet, følger det af persondatalovens § 46, stk. 1, at offentlige myndigheder skal anmelde disse ændringer til Datatilsynet. Såfremt ændringerne er af mindre væsentlig betydning, følger det af bestemmelsens 2. pkt., at disse ændringer imidlertid kan anmeldes efterfølgende, dog senest 4 uger efter iværksættelsen af behandlingen.

Herudover skal offentlige myndigheder i medfør af § 46, stk. 2, indhente Datatilsynets udtalelse til ændringer i de i § 43, stk. 2, nævnte oplysninger, forinden denne ændring iværk-

sættes i behandlingen. Er der tale om en mindre væsentlig ændring, skal der dog alene ske anmeldelse til tilsynet.

Dette gælder ligeledes for private, der i medfør af lovens § 51, stk. 1, skal anmelde ændringer i de i § 48, stk. 2, jf. § 43, stk. 2, nævnte oplysninger til Datatilsynet, forinden ændringerne iværksættes. Såfremt ændringerne er af mindre væsentlig betydning, følger det af bestemmelsens 2. pkt., at disse ændringer imidlertid kan anmeldes efterfølgende, dog senest 4 uger efter iværksættelsen. Herudover skal Datatilsynets tilladelse indhentes, inden ændringerne iværksættes efter § 51, stk. 2. Såfremt ændringerne er af mindre væsentlig betydning, skal der alene ske anmeldelse til Datatilsynet. Anmeldelsen kan endvidere ske efterfølgende, dog senest 4 uger efter iværksættelsen.

5.7.2.3. Krav om udarbejdelse af oversigt over alle behandlinger
Udover anmeldelsespligten er den dataansvarlige forpligtet til at stille de i § 43. stk. 2, nr. 1, 2 og 4-6, nævnte oplysninger om alle de behandlinger af personoplysninger, som udføres for vedkommende, *til rådighed for enhver, som anmoder herom*, jf. persondatalovens § 54, stk. 2. Bestemmelsen har sin baggrund i direktivets artikel 21, stk. 3.

Det betyder, at den dataansvarlige på anmodning har pligt til at udarbejde og inden for rimelig tid udlevere en oversigt over *alle* behandlinger, denne foretager, herunder behandlingsaktiviteter, som ikke er anmeldelsespligtige.

Dette indebærer nødvendigvis – sammen med særligt lovens § 5 – at den dataansvarlige allerede i dag skal have overblik over alle de behandlingsaktiviteter, denne foretager.

5.7.3. Databeskyttelsesforordningen
Ansvarlighed er et gennemgående tema i databeskyttelsesforordningen, idet den dataansvarlige – og i visse tilfælde databehandleren – har ansvaret for, at forordningens regler efterleves i enhver behandlingsaktivitet omfattet af forordningen.

Det fremgår af forordningens artikel 5, stk. 2, at den dataansvarlige er ansvarlig for og skal kunne påvise, at principperne for behandling af personoplysninger i artikel 5, stk. 1, er overholdes. I lighed med gældende ret skal den dataansvarlige således have et overblik over de behandlinger af personoplysninger, som denne foretager for at efterleve forordningens artikel 5, herunder stk. 2.

Det følger af forordningens artikel 24, stk. 1, om den dataansvarliges ansvar, at denne under hensyntagen til behandlingens karakter, sammenhæng, omfang og formål samt sandsynligheden for og graden af de risici, der er for den registreredes rettigheder og frihedsret-

tigheder, skal gennemføre passende tekniske og organisatoriske foranstaltninger og kunne demonstrere, at behandlingen af personoplysninger er i overensstemmelse med forordningen. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

Ansvarligheden kommer således til udtryk ved, at den dataansvarlige både skal efterleve forordningens forskrifter og ligeledes skal være i stand til at påvise, at dette rent faktisk er tilfældet. Dermed er det, i overensstemmelse med gældende ret, op til den dataansvarlige at påvise over for henholdsvis tilsynsmyndigheder og de registrerede personer, at de pågældende behandlingsaktiviteter efterlever forordningens regler. For en nærmere gennemgang af forordningens artikel 24 om den dataansvarliges ansvar henvises til afsnit 5.1.

For netop at påvise, at en behandling overholder forordningens regler, følger det af præambelbetragtning nr. 82, at den dataansvarlige eller databehandleren bør føre fortegnelse over behandlingsaktiviteter under sit ansvar.

Endvidere følger det af præambelbetragtningen, at hver dataansvarlig og databehandler bør have pligt til at samarbejde med tilsynsmyndigheden og efter anmodning stille disse fortegnelser til rådighed for tilsynsmyndigheden, så de kan bruges til at føre tilsyn med behandlingsbetingelserne i forordningen. Den røde tråd i forordningen om ansvarlighed ("accountability") udmøntes således bl.a. i kravet om fortegnelse over behandlingsaktiviteter i forordningens artikel 30.

Et af formålene med kravet om, at dataansvarlige og databehandlere skal føre en fortegnelse, er at bidrage til den samlede dokumentation af, hvordan databeskyttelsesreglerne efterleves. Herudover er det f.eks. et formål, at fortegnelsen kan anvendes i tilsynsmyndighedens arbejde.

Selve forpligtelsen til at føre en fortegnelse følger af forordningens artikel 30. Det fremgår heraf, at den dataansvarlige samt dennes eventuelle repræsentant skal føre fortegnelse over behandlingsaktiviteter under deres ansvar. Endvidere skal databehandlere og deres eventuelle repræsentanter efter bestemmelsen føre fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. I princippet skal de nævnte aktører i en behandling af personoplysninger således, i medfør af forordningens artikel 30, opbevare dokumentation for enhver behandlingsaktivitet.

Fortegnelsen over behandlingsaktiviteter, som føres af den dataansvarlige og databehandleren samt deres eventuelle repræsentanter, skal i medfør af artikel 30, stk. 3, foreligge skriftligt, herunder skal den efter bestemmelsens ordlyd foreligge elektronisk. Forpligtelsen til fortegnelse er således underlagt et formkrav om, at denne ikke *alene* må føres i et fysisk

dokument eller efter hukommelsen. Dette må forstås således, at fortegnelsen kan opbevares elektronisk med henblik på at kunne udprintes i fysisk form, f.eks. med henblik på at udlevere til tilsynsmyndigheden, hvis der anmodes herom.

Herudover følger det af artikel 30, stk. 4, at den dataansvarlige eller databehandleren, samt deres eventuelle repræsentanter, efter anmodning, stiller fortegnelserne til rådighed for tilsynsmyndigheden til brug for de forskellige tilsynsopgaver.

Det er således kun i tilfælde af, at tilsynsmyndigheden anmoder om at få stillet en fortegnelse til rådighed, at den dataansvarlige eller databehandleren skal *udlevere* fortegnelsen. Der er heller ikke en forpligtelse lig den, der følger af persondatalovens § 54, stk. 2.

Desuden kan det bemærkes, at en fortegnelse *ikke* er omfattet af den registreredes ret til indsigt.

Der vil dog for offentlige myndigheders vedkommende, være mulighed for at få aktindsigt i fortegnelser efter de nærmere regler i offentlighedsloven.

Disse to forhold viser netop, at der med forordningens artikel 30 alene skabes en forpligtelse til at udarbejde en *intern* fortegnelse – til erstatning for den eksterne anmeldelse efter gældende ret.

Ved artikel 30 indføres således forpligtelsen for de dataansvarlige og databehandlere til at opbevare intern dokumentation for behandling, der udføres under deres ansvar, i stedet for en generel anmeldelse til tilsynsmyndigheden, som krævet i artikel 18, stk. 1, og artikel 19 i databeskyttelsesdirektivet.

Dette skal ses i lyset af, at formålet med at afskaffe anmeldelsesordningen bl.a. er at erstatte denne med effektive procedurer og mekanismer, som fokuserer på de typer behandlingsaktiviteter, der sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder i medfør af deres karakter, omfang, sammenhæng og formål, jf. præambelbetragtning nr. 89.

5.7.3.1. Den dataansvarliges fortegnelsesforpligtelse

Det følger som nævnt af forordningens artikel 30, stk. 1, at hver dataansvarlig, og hvis det er relevant den dataansvarliges repræsentant, skal føre fortegnelser over behandlingsaktiviteter under deres ansvar. Det må efter bestemmelsens ordlyd antages, at fortegnelsesforpligtelsen efter artikel 30 omfatter al behandlingsaktivitet, det vil sige både behandling af

ikke-følsomme oplysninger efter artikel 6, følsomme oplysninger efter artikel 9 samt oplysninger vedrørende straffedomme og lovovertrædelser efter artikel 10.

Det angives nærmere i artikel 30, stk. 1, litra a-g, hvilke oplysninger der skal være omfattet af fortegnelsen. Den dataansvarlige er naturligvis ikke afskåret fra ved egen drift at dokumentere flere oplysninger, end hvad der følger af kravet i artikel 30, stk. 1, litra a-g.

Der kan i den forbindelse henvises til bilaget nedenfor, hvor der er angivet et eksempel på en fortegnelse over behandlingsaktiviteter i overensstemmelse med forordningens artikel 30, stk. 1.

For det første følger det af stk. 1, *litra a*, at fortegnelsen skal indeholde oplysninger om navn og kontaktoplysninger for den dataansvarlige, og, hvis det er relevant, den fælles dataansvarlige, den dataansvarliges repræsentant og databeskyttelsesrådgiveren. Endvidere skal en eventuel databeskyttelsesrådgiver, som er udpeget på baggrund af forordningens artikel 37 identificeres i fortegnelsen.

Fortegnelseskravet efter litra a, svarer i høj grad til kravet til anmeldelse til tilsynsmyndigheden efter databeskyttelsesdirektivets artikel 19, stk. 1, litra a, og dermed persondatalovens § 43, stk. 2, nr. 1. Til forskel skal den dataansvarlige nu også angive navn og kontaktoplysninger på den fælles dataansvarlige, såfremt der er fælles dataansvar og databeskyttelsesrådgiveren, men ikke oplysningerne på databehandleren.

Dernæst følger det af artikel 30, stk. 1, *litra b*, at fortegnelsen skal omfatte oplysninger om formålene med behandlingen. Det betyder, at samtlige formål med behandlingsaktiviteterne under den dataansvarliges samt dennes repræsentant skal fremgå af fortegnelsen.

Dette krav til fortegnelsen efter litra b, svarer til kravet til fortegnelse i anmeldelse til tilsynsmyndigheden efter direktivets artikel 19, stk. 1, *litra b*, om, at behandlingens formål skal fremgå af en anmeldelse til tilsynsmyndigheden.

Fortegnelsen efter artikel 30 af enhver behandlingsaktivitets formål må i lighed med direktivet skulle forstås på den måde, at der vil kunne formuleres et samlet, logisk sammenhængende formål med en behandling eller en række af behandlinger, som hermed angives som ét formål ud af alle samlede formål hos den dataansvarlige.

Det må således antages, at den dataansvarlige kan samle de behandlingsaktiviteter, som kan formuleres som et samlet, logisk sammenhængende formål, i én fortegnelse over de forskellige behandlingsaktiviteter.

Det betyder, at en privat dataansvarlige vil kunne føre en fortegnelse over forskellige behandlinger med samme formål, såsom f.eks. personaleadministration, kundekartotek, whistleblowerordning mv., i lighed med eksempler fra Datatilsynets fortegnelse over anmeldelser efter gældende ret.[548]

Ligeledes vil en offentlig myndighed kunne samle sine behandlingsaktiviteter under forskellige delformål, såsom behandling af oplysninger i forbindelse med sagsbehandling, pensionsområdet, vielse, beskæftigelse og kommunale ydelser mv. i overensstemmelse med indholdet af de eksisterende fortegnelser i de kommunale fællesanmeldelser i Datatilsynets fortegnelse.

Som et konkret eksempel herpå kan nævnes en kommunes behandling af personoplysninger i forbindelse med beskæftigelse og kommunale ydelser, hvor der vil være flere forskellige delformål, såsom kommunal udbetaling af kommunale ydelser, råd og vejledning, kommunal indsats vedrørende jobformidling mv. I et sådant tilfælde har disse delformål et samlet, logisk sammenhængende formål, som vil kunne angives som kommunens behandling af personoplysninger i forbindelse med dennes forpligtelser inden for beskæftigelse og kommunale ydelser.

Der ses ikke med forordningens artikel 30, stk. 1, litra b, at være tale om et nyt krav til betingelserne for den dataansvarliges behandling af oplysninger, men blot at denne nu udtrykkeligt skal føre en fortegnelse over disse i forvejen definerede formål.

Herudover følger det videre af artikel 30, stk. 1, *litra c*, at der skal indgå en *beskrivelse* af kategorierne af registrerede og kategorier af personoplysninger i fortegnelsen. Dette krav er ligeledes i høj grad lig det, der følger af gældende ret i direktivets artikel 19, stk. 1, litra c og persondatalovens § 43, stk. 2, nr. 5.

Det må således lægges til grund, at dette fortegnelseskrav indebærer en nærmere beskrivelse af, hvilke kategorier af registrerede personer man konkret behandler oplysninger om. Det vil sige, om det f.eks. er oplysninger om nuværende eller tidligere ansatte, kunder, borgere, andre virksomheder mv. Endvidere indebærer beskrivelsen af de typer af oplysninger, der behandles om de registrerede, at det angives, hvilke oplysninger der behandles om disse, såsom f.eks. identifikationsoplysninger, oplysninger om løn, arbejdstid, køb af ydelser mv.

[548] Se Datatilsynets fortegnelse på www.datatilsynet.dk.

Det kan i den forbindelse være relevant at overveje, om det bør fremgå af fortegnelsen, i hvilket omfang der behandles oplysninger om personer i andre medlemsstater. Oplysninger om dette kan bl.a. være relevante, når den dataansvarlige skal finde ud af, hvilken tilsynsmyndighed der har kompetence efter reglen i artikel 56, stk. 1, om ledende tilsynsmyndighed og undtagelsen hertil i artikel 56, stk. 2. Oplysninger om, at der er tale om "et betydeligt antal personer i andre medlemsstater" kan endvidere være nødvendig for tilsynsmyndigheden ved tilrettelæggelse af fælles aktiviteter mellem de nationale tilsynsmyndigheder, jf. forordningens artikel 62.

Der ses ikke med forordningens artikel 30, stk. 1, litra c, at være tale om et nyt krav til betingelserne for den dataansvarliges behandling af oplysninger, men blot at denne nu udtrykkeligt skal føre en fortegnelse over disse i forvejen definerede typer af oplysninger, der behandles om de registrerede personer.

Endvidere følger det af artikel 30, stk. 1, *litra d*, at de kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, herunder modtagere i tredjelande eller internationale organisationer, skal indgå i fortegnelsen. Det må antages, at det alene er de overførsler, der er regelmæssige, der skal anføres i fortegnelsen i overensstemmelse med gældende ret. Dette krav er ligeledes en videreførelse af kravet efter gældende ret, som følger af direktivets artikel 19, stk. 1, litra c, og persondatalovens § 43, stk. 2, nr. 5 og 6.

Forordningens artikel 30, stk. 1, litra d, er dermed ikke udtryk for et nyt krav til betingelserne for den dataansvarliges behandling af oplysninger, men blot at denne nu udtrykkeligt skal føre en fortegnelse over de modtagere, der i forvejen er definerede af den dataansvarlige, som følge af kravet om, at behandling skal tjene et sagligt formål i medfør af forordningens artikel 5, stk. 1, litra b.

Endvidere følger det af artikel 30, stk. 1, *litra e*, at fortegnelsen, hvor det er relevant, skal indeholde oplysning om overførsler af personoplysninger til et tredjeland eller en international organisation og i tilfælde af overførsler i henhold til artikel 49, stk. 1, andet afsnit, dokumentation for passende garantier. For en nærmere gennemgang af forordningens artikel 49 henvises til afsnit 6.6.

Private såvel som offentlige dataansvarlige skal allerede efter gældende ret føre fortegnelse i en eventuel anmeldelse over påtænkte overførsler til tredjelande. Som noget nyt skal fortegnelsen også indeholde oplysninger om overførsler til internationale organisationer, der som en nyskabelse med forordningen, skabes hjemmel til at overføre oplysninger til.

For så vidt angår kravet om, at der skal foreligge dokumentation for passende garantier for overførsler i henhold til artikel 49, stk. 1, følger det allerede af gældende ret, at såfremt en dataansvarlig vil anvende den tilsvarende bestemmelse i persondatalovens § 27, stk. 4, som hjemmelsgrundlag for en tredjelandsoverførsel, skal Datatilsynets tilladelse indhentes. For at opnå denne tilladelse skal den dataansvarlige således efter gældende ret allerede dokumentere de passende garantier, som danner grundlag for et lovligt overførselsgrundlag efter persondataloven. Der er derfor heller ikke for så vidt angår dokumentation for passende garantier, tale om et nyt krav til den dataansvarliges behandling af oplysninger, men blot at denne nu udtrykkeligt skal føre en fortegnelse over disse i forvejen definerede passende garantier.

Herudover følger det af artikel 30, stk. 1, *litra f*, at hvis det er muligt, skal den dataansvarlige angive de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger.

Det er allerede et krav efter gældende ret, at den dataansvarlige skal angive en slettefrist i en anmeldelse til Datatilsynet. Den dataansvarlige skal endvidere efter gældende ret angive starttidspunktet for behandlingen, hvilket er mere omfattende end forordningens krav efter litra f. Dog skal det bemærkes, at det efter forordningen ikke er slettefristen for hele behandlingen, der skal angives i fortegnelsen, men slettefristerne for de forskellige kategorier af oplysninger.

Det følger af imidlertid af forordningens artikel 5, stk. 1, litra e, at personoplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de pågældende personoplysninger behandles. Dermed skal den dataansvarlige i medfør af forordningen til enhver tid vurdere, om det fastsatte saglige formål med behandlingen er opfyldt for at vurdere, om oplysningerne skal slettes. Der er således i forordningens artikel 30, stk. 1, litra f, tale om et krav om kodificering af de overvejelser, som den dataansvarlige i forvejen efter artikel 5, stk. 1, litra f, skal foretage.

Til sidst følger det af artikel 30, stk., 1, *litra g*, at, hvis muligt, skal fortegnelsen indeholde en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i forordningens artikel 32, stk. 1.

Efter gældende ret følger et krav om, at der skal være en generel beskrivelse af de foranstaltninger, der iværksættes af hensyn til behandlingssikkerheden, jf. persondatalovens § 43, stk. 2, nr. 7. I anmeldelser fra offentlige myndigheder skal de dataansvarlige angive, hvorvidt relevante kapitler i sikkerhedsbekendtgørelsen vil blive efterlevet. I anmeldelser fra private virksomheder vil der som oftest medfølge en kortfattet beskrivelse af de sikker-

hedsforanstaltninger, der vil blive truffet. Datatilsynet vil derefter eventuelt følge op med vilkår om datasikkerhed i sin tilladelse til behandlingen.

Forordningens krav herom svarer således – efter sin ordlyd – til det, der følger af gældende ret, idet fortegnelsen dog alene skal indeholde en beskrivelse af sikkerhedsforanstaltningerne, såfremt det er muligt, hvorimod der efter gældende ret altid skal være en sådan beskrivelse i en anmeldelse efter persondataloven.

Herudover kan det bemærkes, at den dataansvarlige og databehandleren i medfør af artikel 32 skal gennemføre en passende sikkerhed for behandlingen af personoplysninger. Den dataansvarlige har således ansvaret for at efterleve forordningens krav til behandlingssikkerhed, men skal samtidig i medfør af artikel 24, stk. 1, kunne påvise, at den dataansvarlige rent faktisk efterlever disse krav i behandlingen af oplysninger. Dermed er det i forvejen op til den dataansvarlige at påvise, at denne har gennemført den nødvendige behandlingssikkerhed i medfør af forordningens artikel 32.

Kravet til fortegnelsen i artikel 30, stk. 1, litra g, er således et krav, der i vidt omfang, allerede følger af gældende ret og forordningen, hvorfor nyskabelsen alene består i, at disse overvejelser skal dokumenteres elektronisk og skriftligt.

Generelt kan det om kravene til en dataansvarliges fortegnelse i medfør af artikel 30, stk. 1, litra a-g, bemærkes, at disse i høj grad er i overensstemmelse med de krav, der for så vidt angår anmeldelsespligtige behandlinger stilles til en dataansvarliges anmeldelse til Datatilsynet for både private og offentlige myndigheder, jf. persondatalovens § 43, stk. 2 og § 48, stk. 2, jf. § 43, stk. 2.

Det kan endvidere bemærkes, at den dataansvarlige allerede på nuværende tidspunkt på anmodning skal være i stand til at udlevere en oversigt til enhver over *alle* behandlingsaktiviteter i medfør af gældende ret i persondatalovens § 54, stk. 2. Som nævnt må det antages, at såfremt den dataansvarlige skal kunne efterleve denne forpligtelse, må den dataansvarlige derfor have et overblik, der kan vises til omverdenen over alle behandlingsaktiviteter. Dog adskiller kravet om fortegnelse sig fra kravet efter persondatalovens § 54, stk. 2, idet fortegnelsen som nævnt er et internt dokument.

Det kan således for så vidt angår kravet i forordningen om fortegnelse af ikke-anmeldelsespligtige behandlinger bemærkes, at der er tale om et krav, der i et vist omfang allerede følger af gældende ret.

Forskellen er, at den dataansvarlige nu efter forordningen altid skal føre fortegnelse over alle behandlingsaktiviteter, hvorimod den dataansvarlige altid skal være forberedt på at udlevere en oversigt over alle behandlinger til enhver, når der anmodes herom efter gældende ret.

5.7.3.2. Databehandlerens fortegnelsesforpligtelse

Som en nyskabelse er databehandleren og dennes eventuelle repræsentant omfattet af kravet om at føre fortegnelse efter forordningens artikel 30, stk. 2. Det følger således af forordningens artikel 30, stk. 2, at hver databehandler, og, hvis det er relevant, databehandlerens repræsentant fører fortegnelser over alle kategorier af behandlingsaktiviteter, der foretages på vegne af en dataansvarlig.

Det betyder, at alle databehandlere er omfattet af forordningens krav om fortegnelse. Dette er en nyskabelse i forhold til gældende ret, hvor databehandlere alene er underlagt anmeldelsesforpligtelsen, når de i medfør af persondatalovens § 53 er etableret i Danmark og udøver edb-servicevirksomhed. Databehandlere skal efter artikel 30, stk. 2, føre fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.

Det følger herefter af artikel 30, stk. 2, litra a-d, hvilke oplysninger databehandlerens fortegnelse skal indeholde. Det følger således af *litra a*, at en databehandlers fortegnelser skal indeholde navn på og kontaktoplysninger på databehandleren eller databehandlerne og hver dataansvarlig, på hvis vegne databehandleren handler, samt, hvis det er relevant, den dataansvarliges eller databehandlerens repræsentant og databeskyttelsesrådgiveren. Dette krav er lig kravet til de dataansvarlige i artikel 30, stk. 1, litra a.

Herudover følger det af artikel 30, stk. 2, *litra b*, at databehandleren skal føre fortegnelse over de kategorier af behandlinger, der foretages på vegne af den enkelte dataansvarlige. Det må lægges til grund, at databehandlerne skal føre fortegnelser over alle de kategorier af behandlinger, som databehandleren behandler på vegne af den dataansvarlige efter forordningens artikel 30, stk. 2, litra b.

Desuden følger det af artikel 30, stk. 2, *litra c*, at databehandleren, hvor det er relevant, skal medtage oplysninger om overførsler af personoplysninger til et tredjeland eller en international organisation, herunder angivelse af dette tredjeland eller denne internationale organisation og i tilfælde af overførsler i henhold til artikel 49, stk. 1, andet afsnit, dokumentation for passende garantier i fortegnelsen.

Det følger af det generelle princip for overførsler i forordningens artikel 44, at der kun må ske overførsel af oplysninger til et tredjeland eller en international organisation, såfremt

betingelserne i kapitel V er opfyldt af den dataansvarlige *og* databehandleren. Som følge heraf, vil databehandleren på baggrund af en dokumenteret instruks fra den dataansvarlige i medfør af artikel 28, stk. 3, litra a, have mulighed for at foretage overførsel af oplysninger til et tredjeland eller en international organisation, såfremt denne stiller fornødne garantier herfor i medfør af artikel 49, stk. 1. Såfremt det er relevant, skal databehandleren således kunne påvise, at betingelserne i artikel 49, stk. 1, er opfyldt. Dermed kan artikel 30, stk. 2, litra c, anses for et krav om dokumentation af en allerede eksisterende forpligtelse for databehandleren.

Dernæst skal databehandleren som følge af *litra d*, hvis det er muligt, medtage en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1, i dennes fortegnelse. Dette krav er lig det, der følger af artikel 30, stk. 1, litra g, for så vidt angår indholdet af den dataansvarliges fortegnelsesforpligtelse.

Det kan her bemærkes, at databehandleren i medfør af artikel 32 er forpligtet til en passende sikkerhed for behandlingen af personoplysninger. Databehandleren har således ansvaret for at efterleve forordningens krav til behandlingssikkerhed for så vidt angår den behandling, der foretages på vegne af den dataansvarlige. Dermed skal databehandleren samtidig være i stand til at påvise, at der er gennemført passende sikkerhedsforanstaltninger i medfør af artikel 32.

Kravet til fortegnelsen i artikel 30, stk. 2, litra d, afspejler således en forpligtelse, databehandleren allerede er underlagt i medfør af forordningens artikel 32, hvorfor nyskabelsen alene består i, at disse overvejelser skal dokumenteres elektronisk og skriftligt.

Generelt kan det bemærkes, at databehandleren som en nyskabelse er forpligtet til at føre fortegnelser over de behandlinger af personoplysninger, som denne foretager på vegne af den dataansvarlige.

5.7.4. Overvejelser

I modsætning til forordningens artikel 30 om fortegnelser over behandlingsaktiviteter følger der ikke en decideret fortegnelsesforpligtelse efter gældende ret.

Det følger imidlertid af anmeldelsespligten i direktivets artikel 18, stk. 1, og persondatalovens §§ 43, stk. 1 og 48, at der ved behandlinger omfattet af disse forpligtelser, skal ske anmeldelse til tilsynsmyndigheden, som indeholder en optegnelse over de behandlingsaktiviteter, der anmeldes.

Der følger således på sin vis et krav om fortegnelser over behandlingsaktiviteter i medfør af anmeldelsesforpligtelsen efter gældende ret.

Hvis en offentlig eller privat dataansvarlig er omfattet af det gældende anmeldelseskrav, vil den dataansvarlige i vidt omfang kunne genanvende de anmeldelser, de har indsendt til Datatilsynet til at føre fortegnelser over behandlingsaktiviteter i medfør af forordningens artikel 30, stk. 1, litra a-g.

Der er således indtil videre ikke holdepunkter for at antage, at fortegnelseskravet efter artikel 30 indebærer krav om at føre skriftlige optegnelser i meget videre omfang, end hvad der kendes fra omfanget af anmeldelserne efter direktivet og persondataloven. Andet ville heller ikke give mening i forhold til tankegangen i præambelbetragtning nr. 89, hvorefter anmeldelsesordningen skal afskaffes, fordi den "medførte en administrative og finansiel byrde".

For så vidt angår de behandlinger, der *ikke* er omfattet af anmeldelsespligten efter gældende ret, vil disse nu i medfør af artikel 30, skulle indgå i en fortegnelse, som omfatter al behandlingsaktivitet under den dataansvarliges ansvar. Også databehandlere pålægges fremover et fortegnelseskrav.

Den dataansvarlige er endvidere i forvejen forpligtet til at udlevere en oversigt over alle behandlinger – inklusiv de behandlingsaktiviteter, der ikke er omfattet af anmeldelsespligten – til enhver, der anmoder herom efter gældende ret i persondatalovens § 54, stk. 2. Dermed er den dataansvarlige i et vist omfang allerede omfattet af krav, der svarer til forordningens krav i artikel 30, dog således at fortegnelse efter artikel 30 alene er et internt dokument.

Der er derfor i praksis tale om en begrænset udvidelse af pligten til fortegnelse i artikel 30 i forhold til gældende ret for den dataansvarlige. Dette skal ses i lyset af, at fortegnelseskravet erstatter den hidtil gældende anmeldelsesordning.

For databehandleren udvides pligten til fortegnelse i artikel 30 i forhold til gældende ret, idet alle behandlingsaktiviteter, herunder dem der alene omfatter behandling af ikkefølsomme oplysninger efter artikel 6, nu efter forordningen skal indgå i de elektroniske og skriftlige fortegnelser hos databehandleren.

Der henvises dog til undtagelsen til kravet om fortegnelser over behandlingsaktiviteter efter forordningens artikel 30, stk. 5.

Endelig er der ikke holdepunkter i forordningen for at antage, at den dataansvarlige og databehandleren skal føre en intern fortegnelse efter en bestemt form, andet end kravet i artikel 30, stk. 3 om, at fortegnelsen skal foreligge skriftligt og elektronisk. Der er således intet til hinder for, at en intern fortegnelse føres i f.eks. et skema eller i et almindeligt (kortere) tekstbehandlingsdokument, der let kan printes og stilles til rådighed for tilsynsmyndigheden, såfremt denne anmoder herom i medfør af artikel 30, stk. 4. Forordningens artikel 30 er ikke tiltænkt som en "belastning" for den dataansvarlige eller databehandleren og medfører ikke i sig selv et krav om udarbejdelse af større analyser af datastrømme mv. Det følger dog som hidtil, at den dataansvarlige skal leve op til princippet om dataminimering i artikel 5, stk. 1, litra c.

Eksempel på en fortegnelse - Dataansvarlig

Eksempel på en fortegnelse over behandlingsaktiviteter vedrørende HR

Dataansvarlig	**Myndighedens/virksomhedens navn, CVR-nr. og kontaktoplysninger** *(adresse, hjemmeside, telefonnummer og e-mail)*	Københavns Kommune Økonomiforvaltningen Rådhuset 1599 København V CVR:
	Den fælles dataansvarlige samt dennes kontaktoplysninger *(adresse, hjemmeside, telefonnummer og e-mail)*	-
	Den dataansvarliges repræsentant samt dennes kontaktoplysninger *(adresse, hjemmeside, telefonnummer og e-mail)* *(Offentlige myndigheder er ikke omfattet, jf. artikel 27, stk. 2, litra b)*	.
	Myndighedens/virksomhedens databeskyttelsesrådgiver samt	DPO, Anders Andersen Kongestien XXX, 1111 Kongsted www.hjemmeside.dk

	dennes kontaktoplysninger *(adresse, hjemmeside, telefonnummer og e-mail)*	+ 45 88 88 88 88 dpo@andersandersen.dk	
Formål (-ene)	**Behandlingens eller behandlingernes formål** *(et samlet, logisk sammenhængende formål med en behandling eller en række af behandlinger, som hermed angives som ét formål ud af alle samlede formål hos den dataansvarlige)*	Personaleadministration	
Kategorierne af registrerede og kategorierne af personoplysningerne	**Kategori af registrerede personer** *(eksempelvis borger/kunder, partsrepræsentanter nuværende eller tidligere ansatte, andre virksomheder, andre myndigheder mv.)*	Der behandles oplysninger om følgende kategorier af registrerede personer: a) Ansøgere b) Ansatte c) Tidligere ansatte d) Pårørende e) Borger der henvender sig til Københavns Kommune f) Politikere	
	Oplysninger, som behandles om de registrerede personer *(afkryds og beskriv de typer af oplysninger, som er omfattet af behandlingsaktiviteterne)*	Oplysninger, som indgår i den specifikke behandling. Beskriv:	
		Identifikationsoplysninger	X
		Oplysninger vedrørende ansættelsesforholdet til brug for administration, herunder stilling og tjenestested, lønforhold, oplysninger af relevans for lønindeholdelse, personalepapirer, uddannelse og sygefravær.	X
		Race eller etnisk oprindelse	
		Politisk, religiøs eller filo-	

		sofisk overbevisning	
		Fagforeningsmæssigt tilhørsforhold	X
		Helbredsoplysninger herunder genetisk data	X
		Biometrisk data med henblik på identifikation	X
		Seksuelle forhold	
		Strafbare forhold	X
Modtagerne af personoplysningerne	**Kategorier af modtagere som oplysninger er eller vil blive videregivet til herunder modtagere i tredjelande og internationale organisationer** *(eksempelvis andre myndigheder, virksomheder, borger/kunder mv.)*	1. Offentlige myndigheder (så vidt muligt myndighedens navn, f.eks. SKAT) 2. Banker 3. Kreditbureauer	
Tredjelande og internationale organisationer	**Oplysninger om overførelse af personoplysninger til tredjelande eller internationale organisationer** *(eksempelvis databehandleres placering i tredjelande, databehandlers brug af cloudløsninger placeret i tredjelande***)**	Nej (*Angivelse af virksomhed/samarbejdspartner, hvis denne er placeret i tredjeland*)	
Sletning	**Tidspunkt for sletning af oplysninger** *(de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger)*	Oplysninger om tidligere ansatte slettes senest X år efter afslutningen af den journalperiode, hvor personalesagen er afsluttet. Oplysninger om ansøgere slettes senest X måneder efter afslutningen af den journalperiode, hvor sagen er afsluttet. Oplysninger overføres løbende til Rigsarkivet efter arkivlovens regler og	

		Statens Arkivers bestemmelser herom.
Tekniske og organisatoriske sikkerhedsforanstaltninger	**Beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger** *(hvis muligt skal der gives en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, jf. artikel 32, stk. 1)*	Behandling af personoplysninger i forbindelse med HR-arbejde sker i overensstemmelse med interne retningslinjer, som bl.a. fastsætter rammerne for autorisation- og adgangsstyring og logning. Personoplysninger opbevares i pseudonymiseret og i kryptret form og transmitteres krypteret. Fysisk materiale opbevares aflåst. Der anvendes følgende sikkerhedsstandarder: ISOXXXXX.

5.8. Fortegnelser over behandlingsaktiviteter – undtagelsen i artikel 30, stk. 5

5.8.1. Præsentation

Det følger af databeskyttelsesforordningens artikel 30, stk. 5, at kravet om fortegnelser over behandlingsaktiviteter i artikel 30, stk. 1 og 2, for henholdsvis dataansvarlige og databehandlere i visse tilfælde kan undtages.

5.8.2. Gældende ret

Der henvises til afsnit 5.7. om fortegnelser over behandlingsaktiviteter efter artikel 30, stk. 1-4.

5.8.3. Databeskyttelsesforordningen

Det følger af databeskyttelsesforordningens artikel 30, stk. 5, at kravet om fortegnelse i artikel 30, stk. 1 og 2, for henholdsvis dataansvarlige og databehandlere i visse tilfælde kan undtages.

Det følger således af artikel 30, stk. 5, at de i artikel 30, stk. 1 og 2, omhandlede forpligtelser ikke finder anvendelse på et foretagende eller en organisation, der beskæftiger under 250 personer, medmindre den behandling, som den foretager, sandsynligvis vil medføre en risiko for registreredes rettigheder og frihedsrettigheder, behandlingen ikke er lejligheds-

vis, eller behandlingen omfatter særlige kategorier af oplysninger, jf. artikel 9, stk. 1, eller personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10.

5.8.3.1. Undtagelsen omhandler alene virksomheder og organisationer
Det følger bl.a. af præambelbetragtning nr. 13, at for at tage hensyn til den særlige situation for mikrovirksomheder og små og mellemstore virksomheder indeholder forordningen en undtagelse for organisationer med mindre end 250 ansatte med hensyn til at føre fortegnelser. Det følger endvidere af præambelbetragtning nr. 13, at begreberne mikrovirksomheder og små og mellemstore virksomheder bør baseres på artikel 2 i bilaget til Kommissionens henstilling 2003/361/EF.

På baggrund af ordlyden i præambelbetragtningen må det antages, at undtagelsesmuligheden ikke omfatter offentlige myndigheder, der i en dansk kontekst forstås i overensstemmelse med afgrænsningen i forvaltningslovens § 1, stk. 1-2, jf. også afsnit 5.18. om offentlige myndigheder og organers forpligtelse til at udpege en databeskyttelsesrådgiver.

Undtagelsen i artikel 30, stk. 5, omhandler efter sin ordlyd kun de dataansvarlige eller databehandlere, der udgør et "foretagende" eller en "organisation".

Et foretagende er defineret i forordningens artikel 4, nr. 18, hvoraf følger, at det er en fysisk eller juridisk person, som udøver økonomisk aktivitet, uanset dens retlige status, herunder partnerskaber eller sammenslutninger, der regelmæssigt udøver økonomisk aktivitet. Der er med andre ord tale om en virksomhed.

Det er ikke i forordningen defineret, hvad der skal betegnes som en "organisation". Der ses i øvrigt ikke at være holdepunkter i forordningen for at antage, at andre aktører end virksomheder (foretagender) ikke skulle kunne påberåbe sig undtagelsen i artikel 30, stk. 5. Dermed må det antages, at f.eks. privatpersoner (eksempelvis en "blogger"), der behandler personoplysninger uden at være omfattet af forordningens artikel 2, stk. 2, litra c, kan være omfattet af undtagelsen i artikel 30, stk. 5.

Herudover er det kun virksomheder og organisationer, der beskæftiger under 250 personer, som er omfattet af undtagelsen i artikel 30, stk. 5. Det må antages, at dette skal beregnes ud fra, hvem der er ansat i den pågældende virksomhed eller organisation.

5.8.3.2. Væsentlige indskrænkninger til undtagelser i artikel 30, stk. 5
Det følger endvidere af artikel 30, stk. 5, at virksomheder og organisationer, der beskæftiger under 250 personer, alligevel ikke er undtaget fortegnelsespligten, hvis den pågælden-

de, konkrete behandlingsaktivitet er omfattet af blot én af tre indskrænkninger nævnt i artikel 30, stk. 5, 2. led.

Efter ordlyden af artikel 30, stk. 5, 2. led, må det i praksis antages, at nogle af en virksomheds eller organisations behandlingsaktiviteter vil kunne undtages fra fortegnelseskravet, mens andre behandlingsaktiviteter ikke kan undtages. Det afgørende er, om den pågældende behandlingsaktivitet omfattes af en af de tre indskrænkninger til undtagelsen, der opregnes i stk. 5, 2. led.

Den første indskrænkning til undtagelsen i artikel 30, stk. 5, 2. led, er behandlingsaktiviteter, der sandsynligvis vil medføre en risiko for registreredes rettigheder og frihedsrettigheder. Det betyder, at graden af risikoen for den registreredes grundlæggende rettigheder og frihedsrettigheder ved en behandling er styrende for, om der kan ske undtagelse fra at føre fortegnelse over behandlingen.

Den anden indskrænkning i stk. 5, 2. led, omfatter behandling foretaget af en virksomhed eller en organisation, der ikke er lejlighedsvis.

Endelig følger det af artikel 30, stk. 5, 2. led, at behandling, der omfatter de særlige kategorier af oplysninger, jf. artikel 9, stk. 1, eller personoplysninger vedrørende straffe og lovovertrædelser, jf. artikel 10, ikke er omfattet af undtagelsen til at føre fortegnelse.

Man skal således som dataansvarlig under alle omstændigheder leve op til fortegnelseskravet i artikel 30, stk. 1-2 – også selvom man beskæftiger under 250 personer – hvis den dataansvarliges behandling af personoplysninger (1) sandsynligvis vil medføre en risiko for registreredes rettigheder og frihedsrettigheder, (2) vil foregå oftere end blot lejlighedsvis, *eller* hvis (3) behandlingen omfatter de særlige kategorier af oplysninger omfattet af forordningens artikel 9, stk. 1, eller artikel 10.

Det må i øvrigt antages at behandling af personoplysninger i forbindelse med sædvanlig personaleadministration under normale omstændigheder ikke vil kunne undtages efter artikel 30, stk. 5, selvom den foregår i virksomheder eller organisationer med under 250 ansatte, da en sådan behandlingsaktivitet må antages normalt at foregå oftere end blot lejlighedsvis.

5.8.4. Overvejelser

Artikel 30, stk. 5, om undtagelse til kravet om fortegnelser over behandlingsaktiviteter i artikel 30, stk. 1, og 2, må i praksis antages at få et meget snævert anvendelsesområde.

Dette skyldes for det første, at det kun er virksomheder og organisationer med under 250 personer beskæftiget, der kan undtages fra fortegnelseskravet. Dernæst skyldes det, at det i medfør af artikel 30, stk. 5, 2. led, er yderst begrænset, hvilke behandlinger der alligevel i sidste ende kan undtages fra kravet om at føre fortegnelse efter artikel 30, stk. 1-2.

5.9. Samarbejde med tilsynsmyndigheden, artikel 31

5.9.1. Præsentation

Når en tilsynsmyndighed skal udføre sine opgaver, bl.a. med at føre tilsyn og håndhæve anvendelsen af forordningen, kan tilsynsmyndigheden være afhængig af at modtage relevant information, og på anden måde at kunne samarbejde med dataansvarlige og databehandlere. Det fremgår af databeskyttelsesforordningens artikel 31, at der skal være et sådant samarbejde. I præambelbetragtning 82 omtales et eksempel på samarbejde bestående i, at dataansvarlige og databehandlere stiller deres fortegnelse over behandlingsaktiviteter til rådighed for tilsynsmyndigheden.

Denne forpligtelse skal ses i sammenhæng med artikel 57 og 58, der behandler tilsynsmyndighedens opgaver og beføjelser.

5.9.2. Gældende ret

Der findes ikke en regel i persondataloven eller i databeskyttelsesdirektivet svarende til databeskyttelsesforordningens artikel 31.

5.9.2.1. Persondatalovens § 62

Af persondatalovens § 62, stk. 1, fremgår, at Datatilsynet kan kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

Persondatalovens § 62, stk. 1, er imidlertid mest sammenlignelig med reglerne i databeskyttelsesforordningens artikel 58, stk. 1, om tilsynsmyndighedens undersøgelsesbeføjelser, herunder artikel 58, stk. 1, litra e, om at tilsynsmyndigheden af den dataansvarlige eller databehandleren skal have adgang til alle personoplysninger og oplysninger, der er nødvendige for at varetage dens opgaver.

Persondatalovens § 62, stk. 1, har sin baggrund i databeskyttelsesdirektivets artikel 28, stk. 3, hvoraf bl.a. fremgår, at hver tilsynsmyndighed skal kunne iværksætte undersøgelser og bl.a. have adgang til de oplysninger, der gøres til genstand for en behandling, og til at indsamle alle oplysninger, der er nødvendige for at varetage dens tilsynsopgaver.

5.9.2.2. Oversigter over behandlinger
Under den gældende persondatalov har Datatilsynet draget nytte af de oversigter over behandlinger, som en dataansvarlig efter persondatalovens § 54, stk. 2, skal stille til rådighed for enhver, som anmoder derom. F.eks. har tilsynet i forbindelse med inspektioner anmodet om at få tilsendt en oversigt over ikke-anmeldelsespligtige behandlinger hos den dataansvarlige.

Ved anvendelse af sin ret til oplysninger efter persondatalovens § 62, stk. 1, har tilsynet også i forhold til databehandlere indhentet oplysninger om, f.eks. hvilke systemer der anvendes, og hvilke underdatabehandlere der benyttes ─ samt hvilke dataansvarlige behandlinger udføres for.

5.9.3. Databeskyttelsesforordningen
5.9.3.1. Databeskyttelsesforordningens artikel 31
Det følger af forordningens artikel 31, at den dataansvarlige og databehandleren samt, hvis det er relevant, deres repræsentanter efter anmodning samarbejder med tilsynsmyndigheden i forbindelse med udførelsen af dens opgaver.

Pligten til at samarbejde er omtalt i en enkelt præambelbetragtning. Det fremgår således af præambelbetragtning nr. 82, at den dataansvarlige eller databehandleren for at påvise overholdelse af denne forordning bør føre fortegnelser over behandlingsaktiviteter under sit ansvar. Hver dataansvarlig og databehandler bør have pligt til at samarbejde med tilsynsmyndigheden og efter anmodning stille disse fortegnelser til rådighed for tilsynsmyndigheden, så de kan bruges til at føre tilsyn med sådanne behandlingsaktiviteter.

5.9.4. Overvejelser
Artikel 31 slår fast, at såfremt tilsynsmyndigheden anmoder om det, skal den dataansvarlige og databehandleren samarbejde med tilsynsmyndigheden. Dette adskiller sig imidlertid ikke væsentlig fra situationen i dag, hvor de dataansvarlige også skal svare på de spørgsmål, som Datatilsynet stiller.

Det i præambelbetragtningen omtalte tilfælde, hvor der vil være behov for samarbejde, må forventes at blive ganske relevant i forhold til tilsynsmyndighedens arbejde med at planlægge og udføre forskellige former for tilsyn, herunder tilsynsbesøg.

Som led i planlægningen af tilsynsaktiviteter vil tilsynsmyndigheden f.eks. kunne foretage screeninger, hvor der fra et antal dataansvarlige indhentes kopi af de fortegnelser over behandlingsaktiviteter, som de dataansvarlige skal føre efter forordningens artikel 30. På baggrund heraf vil tilsynsmyndigheden herefter kunne foretage nærmere planlægning af

sine tilsynsaktiviteter, herunder eventuelle tilsyn som fælles aktiviteter med tilsynsmyndigheder i andre medlemsstater.

5.9.4.1. Behovet for oplysninger
Det må forventes, at samarbejde ─ eventuelt under anvendelse af undersøgelsesbeføjelserne i artikel 58 ─ vil komme på tale i en række forskellige situationer.

Der kan f.eks. være behov for tidligt at indhente oplysninger om en virksomheds etableringer i forskellige medlemslande for at afklare, hvilken tilsynsmyndighed der er kompetent og eventuelt har kompetence som ledende tilsynsmyndighed, jf. forordningens artikel 56, stk. 1.

I den indledede afklaring kan der også være behov for oplysninger om, hvorvidt genstanden for en sag alene vedrører en etablering i Danmark eller alene i væsentlig grad påvirker registrerede i Danmark jf. forordningens artikel 56, stk. 2.

Det kan eventuelt også være relevant at foretage en dialog med en virksomhed om omfanget af registrerede i mere end én medlemsstat med henblik på at afklare, om der er grundlag for at indbyde tilsynsmyndighederne i andre medlemsstater til at deltage i fælles aktiviteter som beskrevet i artikel 62.

5.9.4.2. Oplysninger fra databehandleren
Behovet for samarbejde kan også tænkes at opstå i sager, hvor en databehandler er den eneste part med den nødvendige viden eller den nødvendige adgang til IT-systemerne til at kunne hjælpe med at afklare, hvorledes en hændelse er indtruffet, og hvilke konsekvenser det kan have haft for de behandlede data. I den situation kan det være afgørende, at databehandleren samarbejder med tilsynsmyndigheden om en afklaring af hændelsen, således at tilsynsmyndigheden kan udføre sit arbejde – f.eks. behandle en klage over en konkret databehandling eller en anmeldelse om et brud på datasikkerheden.

5.10. Behandlingssikkerhed, artikel 32

5.10.1. Præsentation
I artikel 32 i databeskyttelsesforordningen er der regler om behandlingssikkerhed i forbindelse med behandling af personoplysninger.

I det følgende gennemgås gældende ret i henhold til persondatalovens § 41, stk. 1-3 og stk. 5 samt § 42. Herefter vil der blive redegjort nærmere for indholdet af databeskyttelsesfor-

ordningens artikel 32, og det vil i tilknytning hertil blive vurderet, hvilke overvejelser forordningens regel om behandlingssikkerhed vurderes at give anledning til med hensyn til forståelsen af gældende ret.

5.10.2. Gældende ret

5.10.2.1. Persondatalovens § 41, stk. 1

Det fremgår af persondatalovens § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, må kun behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Bestemmelsen har sin baggrund i artikel 16 i databeskyttelsesdirektivet, hvoraf det fremgår, at enhver, der udfører arbejde under den dataansvarlige eller databehandleren, herunder databehandleren selv, og som får adgang til personoplysninger, kun må behandle disse efter instruks fra den dataansvarlige, bortset fra tilfælde der er fastsat i lovgivningen.

Det fremgår af bemærkningerne til persondatalovens § 41, stk. 1, at efter bestemmelsen må en person, en virksomhed eller lignende, der udfører en behandling af oplysninger under den dataansvarlige, kun behandle de oplysninger, som vedkommende herigennem får adgang til, i overensstemmelse med instruks fra den dataansvarlige. Bestemmelsen gælder også for en eventuel databehandler.[549]

Endvidere fremgår det af bemærkningerne til persondataloven, at der er ikke særlige formkrav til instrukserne. En instruks kan efter omstændighederne følge af en bestemt stillingsbetegnelse eller af det forhold, at den dataansvarlige autoriserer en ansat eller andre til at have adgang til bestemte oplysninger. Kravet om, at vedkommende person mv. kun må behandle oplysninger i overensstemmelse med instruks fra den dataansvarlige indebærer bl.a., at personen mv. ikke må behandle oplysninger til andre formål end dem, som den dataansvarlige har fastsat – herunder til egne formål – samt at vedkommende ikke må behandle oplysninger efter instruks fra andre end den dataansvarlige. Dette gælder imidlertid ikke, hvis andet følger af lovgivningen.[550]

Det fremgår af persondataloven med kommentarer, at en databehandler, f.eks. et edb-servicebureau, ikke må anvende oplysningerne til noget andet formål end til brug for løsning af netop den opgave, som databehandleren efter aftale med den dataansvarlige har

[549] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 41.
[550] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 41.

påtaget sig. En databehandler vil som følge heraf bl.a. ikke være berettiget til at videregive oplysninger fra et edb-system, som databehandleren varetager driften af, til tredjemand uden instruks herom fra den dataansvarlige.[551]

5.10.2.2. Persondatalovens § 41, stk. 2

Af persondatalovens § 41, stk. 2, fremgår det, at den i stk. 1 omtalte instruks ikke må begrænse den journalistiske frihed eller være til hinder for tilvejebringelsen af et kunstnerisk eller litterært produkt.

Bestemmelsen, der hverken har sin baggrund i databeskyttelsesdirektivet eller Registerudvalgets betænkning nr. 1345 om behandling af personoplysninger, er ifølge bemærkningerne til persondataloven indsat i loven "for at undgå enhver tvivl".[552]

Det fremgår af persondataloven med kommentarer, at det er uklart, hvad der er bestemmelsens praktiske anvendelsesområde. Det må således under alle omstændigheder antages, at personhenførbare oplysninger, jf. § 3, nr. 1, ikke må behandles til andre formål end dem, som den dataansvarlige har fastsat, eller efter instruks fra andre end den dataansvarlige, jf. stk. 1. Hvis det imidlertid falder inden for det fastsatte formål at behandle oplysningerne i journalistisk, kunstnerisk eller litterært øjemed, må instruksen ikke lægge hindringer for den nærmere udøvelse af den journalistiske frihed mv. Samtidig må det antages, at behandlede personoplysninger – uanset instruksen – vil kunne anvendes i ikke-personhenførbar form til f.eks. at tilvejebringe et litterært produkt.[553]

5.10.2.3. Persondatalovens § 41, stk. 3

Databeskyttelsesdirektivets artikel 17, stk. 1, 1. afsnit, fastslår, at medlemsstaterne skal fastsætte bestemmelser om, at den dataansvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for ulovlig behandling.

Af direktivets præambelbetragtning nr. 46 fremgår, at foranstaltningerne skal træffes både under selve udformningen og under iværksættelsen af en behandling.

[551] Persondataloven med kommentarer (2015), s. 547.
[552] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.6.3. i de almindelige bemærkninger.
[553] Persondataloven med kommentarer (2015), s. 547.

Bestemmelsen danner baggrund for persondatalovens *§ 41, stk. 3, 1. pkt.*, hvoraf det fremgår, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Der er tale om en opstilling af de overordnede krav til den dataansvarliges behandlingssikkerhed. Hverken direktivet eller persondatalovens § 41, stk. 3, indeholder således en nærmere beskrivelse af, hvilke typer af foranstaltninger der kan være tale om.

Det fremgår dog af Kommissionens bemærkninger til direktivudkastet af 24. september 1990, at tekniske datasikkerhedsforanstaltninger omfatter: Sikkerhedsforanstaltninger med hensyn til adgang til databehandling og til datalagre, identifikationskoder til personer, der har adgang hertil, edb-sikkerhedsforanstaltninger som f.eks. brug af password for at få adgang til edb-registre, omsættelse af data til kode (kryptering) og kontrol med hacking og andre usædvanlige aktiviteter i edb-registeret. Gennem organisatoriske foranstaltninger skal den dataansvarlige efter Kommissionens bemærkninger tage proceduremæssige skridt inden for den offentlige myndigheds eller erhvervsvirksomheds hierarki, f.eks. ved at etablere forskellige autorisationsniveauer for adgangen til registeret.[554]

På den baggrund finder Registerudvalget i sin betænkning nr. 1345, at sikkerhedsforanstaltninger grundlæggende bør indeholde følgende elementer: Fysisk sikkerhed, organisatoriske forhold, systemtekniske forhold, samt uddannelse og instruktion. Udvalget peger endvidere navnlig på følgende sikkerhedsforanstaltninger, der – alt efter omstændighederne – kan komme på tale: Sikring af bygninger og lokaler, formel autorisation af brugerne, adgangskoder (password), benyttelsesstatistik, logning af transaktioner, registrering af uautoriserede adgangsforsøg, kryptering, regler for udskrifter, regler for destruktion, uddannelse samt tilsyn.[555]

Efter databeskyttelsesdirektivets artikel 17, stk. 1, 2. afsnit, skal der i øvrigt foretages en afvejning af på den ene side det aktuelle tekniske niveau og omkostningerne i forbindelse foranstaltningernes iværksættelse, og på den anden side de risici, som behandlingen indebærer og oplysningstyperne.

Det fremgår endvidere af direktivets præambelbetragtning nr. 10, at gennemførelsen af direktivet ikke må medføre en forringelse af den beskyttelse, som den eksisterende lovgiv-

[554] KOM (90) endelig udgave – SYN 287 og 288, s. 26 f.
[555] Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 325-326.

ning yder, men tværtimod skal formålet være at sikre et højt beskyttelsesniveau overalt i EU.

Registerudvalget forudsætter i sin betænkning nr. 1345 derfor også, at der i forbindelse med gennemførelsen af den nye lovgivning ikke sker en forringelse af det nuværende sikkerhedsniveau, uden at dette nødvendigvis skal opnås på samme måde som i dag.

Der henvises i øvrigt til nedenstående afsnit, hvor bl.a. Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen), og Datatilsynets vejledning nr. 37 af 2. april 2001, som knytter sig til sikkerhedsbekendtgørelsen, er nærmere omtalt.

For en nærmere gennemgang af Datatilsynet praksis på dette område henvises til Datatilsynets årsberetninger og hjemmeside. Siden 2014 har Datatilsynet endvidere hvert år udgivet en række IT-sikkerhedstekster. Formålet med IT-sikkerhedsteksterne, der ligeledes er tilgængelige på tilsynets hjemmeside, er at sætte fokus på udvalgte IT-sikkerhedsmæssige problemstillinger, som dataansvarlige, databehandlere, projektansvarlige og andre i praksis skal håndtere i forbindelse med behandling af personoplysninger.

Fra praksis kan her nævnes, at Datatilsynet i en sag om opbevaring af sikkerhedskopier af e-post over for en e-postserviceudbyder udtalte, at opbevaring i et år lå langt ud over, hvad en almindelig forbruger må formodes at forvente, og derfor ikke fulgte af udbyderens forpligtelser efter § 41, stk. 3.[556]

Endvidere har Datatilsynet i en sag vedrørende Biblioteksstyrelsen og bibliotekernes fremsendelse af elektroniske reserverings- og kvitteringsmeddelelser, der indeholder låneridentifikationsoplysninger og oplysninger om det materiale, låneren har lånt/reserveret, i ikkekrypteret form til de brugere, der ønsker at benytte elektronisk kommunikation med biblioteksvæsenet givet udtryk for den opfattelse, at pligten til at træffe sikkerhedsforanstaltninger efter persondataloven er ufravigelig og ikke bortfalder, selv om den registrerede har givet sit samtykke til det.[557]

Af persondatalovens *§ 41, stk. 3, 2. pkt.,* følger, at pligten til at træffe fornødne tekniske og organisatoriske sikkerhedsforanstaltninger tilsvarende gælder for databehandlere.

[556] Sag om opbevaring af sikkerhedskopier af e-post, Datatilsynets j.nr. 2002-215-0094 (ÅB 2003, s. 113-114).
[557] Biblioteksagen, Datatilsynets j.nr. 2004-082-0188 (ÅB 2005, s. 69 f). Se endvidere om dette spørgsmål om, hvorvidt persondatalovens § 41, stk. 3, er ufravigelig og ikke bortfalder, selv om den registrerede har givet sit samtykke til det, U2005B, s.378 ff, U 2006B, s. 43 ff og U2006B, s. 110-112.

Bestemmelsen må i øvrigt forstås således, at der er tale om en selvstændig pligt for databehandlere til at sørge for, at kravene i § 41, stk. 3, bliver overholdt i forbindelse med behandlingen. Databehandlerens forpligtelser er således ikke begrænset til den aftale, der er indgået mellem den dataansvarlige og databehandleren.[558]

Databehandlerens forpligtelser gælder, uanset om der er tale om en databehandler, der foretager behandling af oplysninger for en dataansvarlig, der er etableret i eller uden for Danmark, herunder i en anden medlemsstat. Hvis databehandleren udøver sin virksomhed på dansk område, gælder reglen om behandlingssikkerhed.[559]

En dataansvarlig, der er etableret i Danmark, og som er en del af den offentlige forvaltning, skal derfor sikre sig, at databehandleren iagttager reglerne i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen), uanset om behandlingen udføres af et edb-servicebureau, der er etableret i en anden medlemsstat.

5.10.2.4. Persondatalovens § 41, stk. 4

Ifølge persondatalovens § 41, stk. 4, skal der for oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Bestemmelsen, der indeholder den såkaldte "krigsregel", vil ikke blive nærmere gennemgået dette sted. Der henvises i stedet til afsnit 5.15. om krigsreglen.

5.10.2.5. Persondatalovens § 41, stk. 5

Det fremgår af persondatalovens § 41, stk. 5, at justitsministeren kan fastsætte nærmere regler om sikkerhedsforanstaltninger. Bestemmelsen har ikke sin baggrund i databeskyttelsesdirektivet, og den fandtes heller ikke i de tidligere gældende registerlove.

I den offentlige sektor var de mere detaljerede krav til datasikkerheden oprindelig fastsat i såkaldte registerforskrifter, som bortfaldt samtidig med persondatalovens ikrafttræden. Da det ikke blev anset for praktisk muligt i lovteksten at angive de nærmere sikkerhedsforanstaltninger, som skal iværksættes i de forskellige sektorer, valgte man på den baggrund at indsætte bemyndigelsesbestemmelsen i stk. 5.

[558] Persondataloven med kommentarer (2015), s. 549.
[559] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 41.

Af bemærkningerne til persondataloven fremgår, at der ved fastsættelsen af de nærmere regler om behandlingssikkerhed bør tages udgangspunkt i (den tidligere) praksis i henhold til registerlovene. Der blev herved bl.a. lagt vægt på præambelbetragtning nr. 10, jf. ovenfor.

Endvidere er det i bemærkningerne forudsat, at der ved fastsættelsen af reglerne – præcis som det er tilfældet ved persondatalovens § 41, stk. 3 – skal foretages en afvejning af det aktuelle tekniske niveau og omkostningerne i forbindelse med iværksættelsen af sikkerhedsforanstaltningerne på den ene side, og de risici, som behandlingen indebærer, og arten af de oplysninger, der behandles, på den anden side, jf. ovenfor om direktivets artikel 17, stk. 1, 2. afsnit.

Det fremgår herudover af de almindelige bemærkninger til persondataloven, at det var hensigten ved lovens ikrafttræden at udstede en bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning helt eller delvis ved hjælp af elektronisk databehandling. Endvidere var det forudsat, at der skulle udstedes en tilsvarende bekendtgørelse for domstolene. Derimod var det ikke en forudsætning, at der (straks) ved lovens ikrafttræden skulle fastsættes nærmere regler om behandlingssikkerheden i den private sektor.[560]

Med hjemmel i bestemmelsen har Justitsministeriet udstedt bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen). Sikkerhedsbekendtgørelsen, der efterfølgende er blevet ændret ved bekendtgørelse nr. 201 af 22. marts 2001, blev i sin tid i øvrigt udarbejdet med udgangspunkt i Registertilsynets cirkulære af 23. februar 1989 om sikkerhedsforanstaltninger for pc- og terminalanvendelse mv. Datatilsynet har endvidere udarbejdet en vejledning, som knytter sig til den oprindelige bekendtgørelse.[561]

Sikkerhedsbekendtgørelsen gælder ifølge bekendtgørelsens § 1 for behandlingen af personoplysninger, som foretages for den offentlige forvaltning helt eller delvis ved hjælp af elektronisk behandling.

Hvilke regler, der skal efterleves i sikkerhedsbekendtgørelsen, afhænger herefter af, om de behandlede oplysninger er omfattet af anmeldelsespligten til Datatilsynet. Efter bekendtgørelsens § 2 skal behandling af personoplysninger således som udgangspunkt alene ske i

[560] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.7.2. i de almindelige bemærkninger.
[561] Datatilsynets vejledning nr. 37 af 2. april 2001

overensstemmelse med bestemmelserne i (bekendtgørelsens) kapitel 1 (§§ 1-4) og kapitel 2 (§§ 5-14).

Behandling af personoplysninger, hvor der skal ske anmeldelse til Datatilsynet efter reglerne i kapitel 12 i persondataloven, skal imidlertid ifølge bekendtgørelsens § 2 og § 15 tillige ske i overensstemmelse med bestemmelserne i bekendtgørelsens kapitel 3 (§§ 15-19), medmindre der er tale om behandling af personoplysninger, der udelukkende sker med henblik på at føre et retsinformationssystem, i det omfang der er tale om oplysninger i den offentligt tilgængelige del af retsinformationssystemet, eller behandling af oplysninger om ansattes fagforeningsmæssige tilhørsforhold i forbindelse med aftaler om kontingentindeholdelse.

Det følger af bekendtgørelsens § 3, der som nævnt er placeret i bekendtgørelsens kapitel 1, og som alle behandlinger skal ske i overensstemmelse med, jf. § 2, stk. 1, at den dataansvarlige myndighed skal træffe de fornødne tekniske og organisatoriske foranstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.

Bestemmelsen er en gentagelse af persondatalovens § 41, stk. 3, idet dog sidste punktum ikke er medtaget.

Uanset de øvrige og mere specifikke bestemmelser i sikkerhedsbekendtgørelsen er den dataansvarlige myndighed således under alle omstændigheder ansvarlig for sikringen af, at der træffes de nævnte fornødne sikkerhedsforanstaltninger. Med andre ord kan en dataansvarlig myndighed ikke ved "blot" at overholde de generelle sikkerhedsbestemmelser i bekendtgørelsens kapitel 2 og de supplerende sikkerhedsforanstaltninger i kapitel 3 uden videre gå ud fra, at sikkerhedskravene i persondatalovens § 41, stk. 3, er overholdt.

Der kan i den forbindelse henvises til, at det i vejledningen til sikkerhedsbekendtgørelsen om netop bekendtgørelsens § 3 anføres, at "[e]n mere generelt dækkende vejledning om etablering af såvel tekniske som organisatoriske sikkerhedsforanstaltninger i forbindelse med elektronisk databehandling kan findes i Dansk Standard DS 484, Norm for edb-sikkerhed."[562] Denne standard er nu afløst af informationssikkerhedsstandarden ISO 27001, som alle statslige myndigheder skal følge, og alle andre offentlige myndigheder skal følge principperne i.[563] Under alle omstændigheder fremgår det dog implicit, men ty-

[562] Datatilsynets vejledning nr. 37 af 2. april 2001.
[563] Den fælles offentlige digitaliseringsstrategi for 2016-2020.

deligt af den citerede vejledningstekst, at de øvrige bestemmelser i sikkerhedsbekendtgørelsen ikke kan stå alene.

Der kan i den forbindelse også henvises til bekendtgørelsens § 14, hvorefter der kun må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger. Det fremgår af vejledningen hertil bl.a., at "[d] særlige sikkerhedsforanstaltninger skal træffes efter myndighedens vurdering af sikkerhedsrisici i det konkrete tilfælde, herunder med hensyntagen til karakteren af de omhandlede oplysninger. For at kunne fastlægge sikkerhedsniveauet er det nødvendigt, at den dataansvarlige foretager en samlet risikovurdering, som omfatter alle elementer i kommunikationsforbindelsen." Det fremgår også i vejledningen vedrørende § 14 om sikkerhedsforanstaltninger ved transmission af oplysninger over det åbne internet, at "[d]isse risici må vurderes af den dataansvarlige i den konkrete situation, således at der kan træffes de fornødne sikkerhedsforanstaltninger."

Endelig kan der henvises til sikkerhedsbekendtgørelsens § 4, hvorefter Datatilsynet – i forbindelse med sit tilsyn med overholdelsen af sikkerhedsbekendtgørelsen – kan komme med henstillinger over for den dataansvarlige myndighed vedrørende de trufne sikkerhedsforanstaltninger, som myndigheden træffer efter § 3.

Sikkerhedsbekendtgørelsen skal således ikke anses for at være udtømmende, men må nødvendigvis bl.a. suppleres af den dataansvarlige myndigheds risikobaserede overvejelser om, hvad der skal udgøre de fornødne sikkerhedsmæssige foranstaltninger i det konkrete tilfælde for at sikre, at personoplysninger ikke hændeligt eller ulovligt tilintetgøres, fortabes eller forringes eller kommer til uvedkommendes kendskab misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.

Kapitel 2 i bekendtgørelsen indeholder regler om udarbejdelse og kontrol af uddybende sikkerhedsregler (§ 5), instruktion af medarbejdere (§ 6), databehandleraftaler (§ 7, stk. 1), pc-arbejdspladser uden for den dataansvarlige myndigheds lokaliteter (§ 7, stk. 2), sikring af de fysiske rammer (§ 8), reparation og service af dataudstyr, herunder salg og kassation af anvendte datamedier (§ 9), ind- og uddatamateriale, som indeholder personoplysninger (§ 10 og § 13), autorisation og adgangskontrol (§ 11) og eksterne kommunikationsforbindelser (§ 14).

Bekendtgørelsens kapitel 3 indeholder som nævnt en række supplerende sikkerhedsforanstaltninger for anmeldelsespligtige behandlinger. Det drejer sig om regler om autorisation og adgangskontrol (§§ 16-§ 17), kontrol med afviste adgangsforsøg (§ 18) og logning (§ 19).

Der er endvidere med hjemmel i § 41, stk. 5, udstedt bekendtgørelse nr. 535 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for domstolene. Bekendtgørelsen afviger kun på få punkter fra sikkerhedsbekendtgørelsen.

Justitsministeren har derimod endnu ikke benyttet bemyndigelsesbestemmelsen til at fastsætte nærmere regler om sikkerhedsforanstaltninger i den private sektor. For den private sektor er det derfor rammebestemmelsen i persondatalovens § 41, stk. 3, der gælder.

Det fremgår imidlertid af persondataloven med kommentarer, at det vil være naturligt, at man som udgangspunkt stiller de samme krav til den mere detaljerede udmøntning af datasikkerheden i private virksomheder mv. som i forhold til den offentlige forvaltning, såfremt forholdene i øvrigt kan sammenlignes. Datatilsynet har hidtil udtalt sig på linje hermed.[564]

Fra praksis kan i den forbindelse således nævnes, at Datatilsynet i en sag om sikkerhedsbrud og optagelse af kundesamtaler hos Natur-Energi A/S, generelt opfordrede selskabet til i videst muligt omfang at tilrettelægge sikkerhedsforanstaltningerne omkring de behandlinger af personoplysninger, som Natur-Energi A/S er dataansvarlig for, i overensstemmelse med sikkerhedsbekendtgørelsen for den offentlige forvaltning.[565]

Endvidere kræver visse behandlinger i den private sektor en tilladelse fra Datatilsynet, jf. persondatalovens § 50, stk. 1 og 2. Datatilsynet har i forbindelse med disse tilladelser til private dataansvarlige mulighed for at fastsætte nærmere vilkår for udførelsen af behandlingerne til beskyttelse af de registreredes privatliv, herunder krav om bestemte sikkerhedsforanstaltninger, jf. § 50, stk. 5. Tilsynet har f.eks. stillet krav om sikkerhedsforanstaltninger til privathospitaler.[566]

Datatilsynets har endvidere fastsat en række krav og anbefalinger i forbindelse med overførsel af personoplysninger via internettet for den private sektor.[567]

5.10.2.6. Persondatalovens § 42, stk.1

Af persondatalovens § 42, stk. 1, fremgår, at når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger og påse, at dette sker.

[564] Persondataloven med kommentarer (2015), s. 556.
[565] Datatilsynets j.nr. 2013-631-0053.
[566] Se Datatilsynets ÅB 2008 og 2009.
[567] Disse kan læses på Datatilsynets hjemmeside.

Bestemmelsen har sin baggrund i databeskyttelsesdirektivets artikel 17, stk. 2, hvorefter medlemsstaterne fastsætter bestemmelser om, at den dataansvarlige, hvis oplysninger behandles for dennes regning, skal vælge en databehandler, som frembyder den fornødne garanti med hensyn til de tekniske sikkerhedsforanstaltninger og organisatoriske foranstaltninger, der skal træffes, og skal påse, at disse foranstaltninger overholdes.

Hvis behandlingen af personoplysninger overlades til en databehandler, pålægger bestemmelsen, at den dataansvarlige skal sikre sig, at databehandleren også opfylder kravene til behandlingssikkerhed i § 41, stk. 3-5, herunder også bestemmelser i sikkerhedsbekendtgørelsen, hvis der er tale om behandling for den offentlige forvaltning. Endvidere pålægger bestemmelsen den dataansvarlige at føre kontrol med, at databehandleren træffer de nødvendige sikkerhedsforanstaltninger.

Kravet om, at den dataansvarlige skal føre kontrol med databehandleren, indebærer i øvrigt, at den dataansvarlige ikke blot kan overlade det til edb-servicebureau, under tilsyn af Datatilsynet, at sikre datasikkerheden, men selv aktivt skal påse, at den fornødne datasikkerhed iagttages.[568]

Fra praksis kan nævnes en sag vedrørende salg af brugt edb-udstyr, hvor Datatilsynet bemærkede over for en virksomhed, som havde overladt det til en databehandler at slette personoplysninger fra harddiskene, hvilket ikke var sket, at det havde været rigtigst, om der fra den dataansvarliges side var blevet udført en vis kontrol med sletningen, f.eks. i form af stikprøver.[569]

5.10.2.7. Persondatalovens § 42, stk. 2

Efter persondatalovens § 42, stk. 2, skal gennemførelse af en behandling ved en databehandler ske i henhold til en skriftlig aftale parterne imellem. Af aftalen skal det fremgå, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren. Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne.

Kravet om skriftlig aftale parterne imellem, gælder efter bestemmelsens ordlyd enhver situation, hvor en databehandling foretages af en databehandler på den dataansvarliges

[568] Persondataloven med kommentarer (2015), s. 571.
[569] Datatilsynets j.nr. 2000-631-0057 og 2001-631-0062 (ÅB 2001, s. 69-70)

vegne. Bestemmelsen omfatter dermed ikke alene overladelse af en behandling til et edb-servicebureau, men også databehandling hos f.eks. en selvstændig konsulentvirksomhed.[570]

Bestemmelsen har sin baggrund i databeskyttelsesdirektivets artikel 17, stk. 3 og 4. Det følger således af direktivets artikel 17, stk. 3, at gennemførelse af en behandling ved en databehandler skal ske i henhold til en kontrakt eller et andet retligt bindende dokument mellem databehandleren og den dataansvarlige, hvori det navnlig fastsættes, at databehandleren alene handler efter instruks fra den dataansvarlige, og at forpligtelserne i henhold til stk. 1, som fastlagt i lovgivningen i den medlemsstat, hvor databehandleren er etableret, ligeledes påhviler denne.

Endvidere fremgår det af direktivets artikel 17, stk. 4, at de dele i kontrakten eller det retlige dokument, der vedrører beskyttelse af oplysninger, og de krav, der vedrører de i stk. 1 omhandlede foranstaltninger med henblik på opbevaring af beviserne, skal foreligge skriftligt eller i anden tilsvarende form.

Der henvises endvidere til afsnit 5.5. om forordningens artikel 28, databehandler.

5.10.3. Databeskyttelsesforordningen

5.10.3.1. Databeskyttelsesforordningens artikel 32, stk. 1

Det fremgår af forordningens artikel 32, stk. 1, at under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstalt-ninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant de i litra a - d nævnte foranstaltninger.

For så vidt angår det i artikel 32, stk. 1, indeholdte begreb "frihedsrettigheder" henvises til afsnit 2.1. om artikel 2 og 3, anvendelsesområde.

Af præambelbetragtning nr. 83 fremgår endvidere, at for at opretholde sikkerheden og hindre behandling i strid med denne forordning bør den dataansvarlige eller databehandleren vurdere de risici, som en behandling indebærer, og gennemføre foranstaltninger, der kan begrænse disse risici, som f.eks. kryptering. Disse foranstaltninger bør under hensyntagen til det aktuelle tekniske niveau og implementeringsomkostningerne sikre et tilstrækkeligt sikkerhedsniveau, herunder fortrolighed, i forhold til risiciene og karakteren af de person-

[570] Persondataloven med kommentarer (2015), s. 572.

oplysninger, der skal beskyttes. Ved vurderingen af datasikkerhedsrisikoen bør der tages hensyn til de risici, som behandling af personoplysninger indebærer, såsom hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, og som navnlig kan føre til fysisk, materiel eller immateriel skade.

Som det første eksempel på en foranstaltning, som det kan være relevant at gøre brug af i sikkerhedsmæssige sammenhænge, nævnes i forordningens artikel 32, stk. 1, litra a, begreberne *pseudonymisering og kryptering* af personoplysninger.

Særligt for så vidt angår begrebet pseudonymisering gælder, at dette er nærmere defineret i artikel 4, nr. 5. Det fremgår således af denne bestemmelse, at med pseudonymisering menes behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person.

Endvidere fremgår af præambelbetragtning nr. 28, at anvendelsen af pseudonymisering af personoplysninger kan mindske risikoen for de berørte registrerede og gøre det lettere for dataansvarlige og databehandlere at opfylde deres data-beskyttelsesforpligtelser. Det er ikke tanken med den udtrykkelige indførelse af "pseudonymisering" i denne forordning at udelukke andre databeskyttelsesforanstaltninger.

Kryptering er omsættelse af data til kode og kan anvendes som en foranstaltning, der, hvis den er behørigt implementeret, kan mindske risikoen for manglende fortrolighed, integritet, uafviselighed og autentifikation.[571]

I forordningens artikel 32, stk. 1, litra b, peges endvidere på en anden mulig foranstaltning i form af *evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester.*

Med udtrykket *integritet* sigtes bl.a. til, at det er muligt at validere, om data på disse systemer er korrekte, pålidelige, nøjagtige og/eller fuldstændige.

For så vidt angår behandlingssystemer og -tjenesters *tilgængelighed* sigtes bl.a. til, at behandlingssystemer og -tjenester og data i disse er tilgængelige ved anmodning fra autorise-

[571] Se endvidere DS/ISO/IEC 27002, 3. udgave, afsnit 10.1.1.

ret bruger, eksempelvis ved at sikre en velfungerende backup eller dublerede systemer alt afhængig af, om det er relevant. Det er normalt en forudsætning, at der er fastlagt organisatoriske processer for, hvorledes disse opgaver udføres, og hvordan f.eks. backup testes.

Med udtrykket *robusthed* sigtes bl.a. til at sikre behandlingssystemer og -tjenesters tekniske og organisatoriske modstandsdygtighed, f.eks. ved at sikre dem imod skadelige hændelser. Der kan f.eks. sikres imod udfald ved dublerede diske, køling, nødstrømsanlæg, automatisk brandslukning, mv. alt afhængig af, om det er relevant.

Med udtrykket *vedvarende* menes, at evnen til at sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester ikke blot skal opfyldes én gang, men er en løbende teknisk og organisatorisk forpligtelse.

Endvidere fremgår det af forordningens artikel 32, stk. 1, litra c, at en anden foranstaltning, der kan komme på tale, er *evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse*.

Der sigtes hermed til, at organisationen har et beredskab for, hvordan adgangen til personoplysninger genoprettes i tilfælde af hændelser som f.eks. brand, hacking, ransomware eller overgravede datakommunikationskabler. Det kan kræve, at organisationen har planlagt, hvorledes IT-driften i pågældende tilfælde kan genoprettes inden for et nærmere bestemt tidsrum, f.eks. ved brug af backup eller overgang til alternative datakommunikationslinjer alt afhængig af, om det er relevant. Evnen til rettidig genoprettelse kan f.eks. demonstreres ved øvelser og test.

I forordningens artikel 32, stk. 1, litra d, peges endelig på foranstaltningen en *procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed*.

Det sigtes hermed til f.eks. med jævne mellemrum at teste/afprøve, vurdere og evaluere – alt afhængig af om det er relevant – firewalls, krypterede forbindelser, krypterede lagringer, foranstaltninger imod forsøg på overbelastelsesangreb, foranstaltninger imod forsøg på at gætte adgangsgivende faktorer, adgangskontrol, brugeradministrationsprocessen og meget andet.[572]

[572] Se f.eks. DS/ISO/IEC 27001:2013 anneks A, fx A.17.1.1 - A.17.1.3.

Afslutningsvis skal det bemærkes, at som det fremgår af ordlyden af artikel 32, stk. 1, kan den dataansvarlige også leve op til bestemmelsen ved brug af *organisatoriske foranstaltninger*.

Sådanne organisatoriske foranstaltninger vil eksempelvis kunne være, at en arbejdsplads begrænser medarbejdernes adgang til personoplysninger, således at det kun er bestemte medarbejdere, som har adgang til f.eks. følsomme personoplysninger.

Det fremgår, som anført af forordningens artikel 32, stk. 1, at der skal tages hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, når der fastsættes passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

Et eksempel på en situation, hvor denne afvejning af hensyn kommer i fokus, vil være, når et ældre systems sikkerhed skal gennemgås. Viser det sig i et sådant tilfælde, at systemet ikke på alle områder helt modsvarer det aktuelle tekniske niveau,[573] men at implementeringsomkostningerne ved at bringe hele systemet på niveau er uforholdsmæssigt store, kan den dataansvarlige i stedet søge at imødekomme behovet for større sikkerhed ved hjælp af også organisatoriske foranstaltninger. Der er således ingen forpligtelse til at efterkomme sikkerhedskravene alene rent teknisk, såfremt der efter en konkret vurdering fra den dataansvarlige findes tilstrækkelige organisatoriske løsninger, der også kan bidrage til at sikre det aktuelle tekniske niveau. Kan der etableres et passende sikkerhedsniveau for allerede ibrugtagne ældre systemer også gennem interne procedurer, undervisning af ansatte eller tilsvarende organisatoriske foranstaltninger, vil dette i princippet kunne være tilstrækkeligt.

5.10.3.2. Databeskyttelsesforordningens artikel 32, stk. 2

Ved vurderingen af, hvilket sikkerhedsniveau der er passende, skal der ifølge forordningens artikel 32, stk. 2, navnlig tages hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er videregivet, opbevaret eller på anden måde behandlet.

Bestemmelsen i stk. 2 kan betragtes som en vejledning til den dataansvarlige angående, hvilke risici der *navnlig* skal tages hensyn til, når sikkerhedsniveauet efter stk. 1 fastsættes. Der er dermed ikke tale om en udtømmende liste over potentielt relevante hensyn.

[573] Begrebet skal forstås i overensstemmelse med den engelske sprogversion, hvor der står "*state of the art"*. "*Det aktuelle niveau"* forstås derfor som *"det højest mulige niveau"*.

5.10.3.3. Databeskyttelsesforordningens artikel 32, stk. 3
Efter forordningens artikel 32, stk. 3, kan overholdelse af et godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 bruges som et element til at påvise overholdelse af kravene i stk. 1.

5.10.3.4. Databeskyttelsesforordningens artikel 32, stk. 4
Det fremgår af forordningens artikel 32, stk. 4, at den dataansvarlige og databehandleren tager skridt til at sikre, at enhver fysisk person, der udfører arbejde for den dataansvarlige eller databehandleren, og som får adgang til personoplysninger, kun behandler disse efter instruks fra den dataansvarlige, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

5.10.4. Overvejelser
Forordningens artikel 32, stk. 1 og 2, har i meget vidt omfang identisk ordlyd med artikel 17, stk. 1, i databeskyttelsesdirektivet. Som anført ovenfor under gældende ret er persondatalovens § 41, stk. 3, baseret på denne bestemmelse i databeskyttelsesdirektivet, hvorfor der er en formodning for, at bestemmelserne har samme indholdsmæssige betydning, herunder samme krav til sikkerhedsniveauet, jf. dog umiddelbart nedenfor.

Det er imidlertid i forhold til databeskyttelsesdirektivet en nyskabelse, når forordningens artikel 32, stk. 1, som nævnt ovenfor, kommer med en nærmere beskrivelse af, hvilke typer af foranstaltninger der bl.a. kan komme på tale at gøre brug af i sikkerhedsmæssige sammenhænge.

Som bestemmelsen er formuleret, fremstår litra a-d i øvrigt ikke som en udtømmende liste over potentielt relevante foranstaltninger, og litra a-d udelukker dermed ikke, at der skal træffes yderlige foranstaltninger for at sikre efterlevelse af artikel 32, stk. 1. Bestemmelsen indebærer heller ikke, at alle de nævnte foranstaltninger skal gennemføres. Litra a-d fremstår som eksempler på foranstaltninger, der skal gennemføres under hensyntagen til blandt andet *risici*, og hvis det er *relevant*.

Opregningen i litra a-d vil efter den 25. maj 2018, hvor forordningen finder anvendelse, i øvrigt være det tætteste, det er muligt at angive, hvilke nærmere sikkerhedsforanstaltninger, som det bl.a. kan komme på tale at anvende i sikkerhedsmæssige sammenhænge.

Det vurderes således ikke muligt at opretholde den i persondatalovens § 41, stk. 5, indeholdte bemyndigelsesbestemmelse, hvorefter justitsministeren kan fastsætte nærmere generelle regler om sikkerhedsforanstaltninger.

Med databeskyttelsesforordningen lægges der imidlertid også op til at sætte en på mange måder – i hvert fald set med danske øjne – ny ramme for og tilgang til behandlingssikkerhed.

Den risikobaserede tilgang er kommet mere i fokus, jf. dog det ovenfor anførte om persondatalovens § 41, stk. 5, hvoraf det fremgår, at selv for dataansvarlige myndigheder, som er bundet af udmøntningen af sikkerhedskravene i sikkerhedsbekendtgørelsen, er der ikke med bekendtgørelsen tale om en udtømmende regulering af, hvilke sikkerhedsforanstaltninger der er tilstrækkelige. Det er således ikke alene private dataansvarlige, men i et vist omfang også dataansvarlige myndigheder, der allerede i dag skal foretage risikobaserede overvejelser for at fastlægge det rette sikkerhedsniveau.

Udgangspunktet efter forordningen er således, at behandling af personoplysninger er forbundet med risici for fysiske personer rettigheder og frihedsrettigheder. Princippet er herefter, at der skal etableres et sikkerhedsniveau, som passer til disse risici ved hjælp af passende tekniske og organisatoriske foranstaltninger, som skal gennemføres af den dataansvarlige og databehandlere.

Forordningen foreskriver ikke, hvilke præcise foranstaltninger der skal træffes. Valget ligger ifølge forordningens artikel 32 i første række hos den dataansvarlige og eventuelle databehandlere. Den dataansvarlige er ansvarlig for og skal kunne påvise og dokumentere, at personoplysninger behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger. For at kunne gøre dette, er den dataansvarlige nødt til at afdække risici forbundet med behandlingen i en risikoanalyse, samt gennemføre dokumenterede foranstaltninger. Der kan i denne forbindelse henvises til artikel 5, stk. 1, litra f, jf. artikel 5, stk. 2, og til artikel 30 stk. 1, litra g.

Af Peter Blumes bog om persondataforordningen fremgår i øvrigt bl.a., at:

> "Risikoorientering er et af de nye træk ved forordningen. Risiko er i sig selv et fremtidssikret begreb. Det tager sigte på noget, som kan ske og som bør undgås. Ved at tillægge risiko betydning bliver persondataretten proaktiv eller har i hvert fald mulighed for at blive det. Risikoorientering tilfører persondataretten noget dynamisk, der kan være krævende for både de dataansvarlige og tilsynsmyndighederne, men kan underbygge god databeskyttelse."[574]

[574] Peter Blume, Den nye persondataret (2016), s. 206-208.

Det må formodes, at databeskyttelsesforordningens risikobaserede tilgang til behandlingssikkerhed i praksis vil kunne facilitere en højnelse af behandlingssikkerheden sammenlignet med, hvad der opnås med persondatalovens regler og sikkerhedsbekendtgørelsen. Foranstaltninger, der etableres, må endvidere formodes at blive etableret målrettet mod de afdækkede risici.

En risikobaseret tilgang kan formentlig i nogle situationer dog ende med at angive et behov for et lavere niveau af beskyttelse af data eller en anderledes metode til beskyttelse af data, end hvad der følger af kravene i sikkerhedsbekendtgørelsen i dag.

En risikobaseret tilgang til sikkerhed kendes allerede i dag i form af for eksempel informationssikkerhedsstandarden ISO 27001, som alle statslige myndigheder skal følge, og alle andre offentlige myndigheder skal følge principperne i.[575] Standarden beskriver kravene til et dækkende informationssikkerheds-ledelsessystem (ISMS), som skal sikre en risikobaseret, effektiv og fleksibel styring af sikkerheden.

Den risikobaserede tilgang kendes også fra ISO/IEC DIS 29134 *"Information technology – Security techniques – Privacy impact assesment – Guidelines"*. Der er tale om en international standard vedrørende privacy impact assesments udarbejdet af den internationale standardiseringsorganisation.[576] ISO 29134 standarden er en vejledning i, hvorledes en Privacy Impact Assessment proces (analogt en konsekvensanalyse) kan udføres. Standarden beskriver processen i en række trin, hvoraf et trin f.eks. vedrører identifikation af risici og et senere trin f.eks. vedrører beslutning om foranstaltninger. Standarden sætter bl.a. fokus på, at behandlingssikkerhed bliver iagttaget og indarbejdet i f.eks. design og implementeringen af IT-løsninger. ISO 29134 standarden vedrører privacy impact assessment. Det må antages, at de europæiske tilsynsmyndigheder og Databeskyttelsesrådet også vil tage standarden i betragtning i forbindelse med overvejelser om forordningens bestemmelser om behandlingssikkerhed og beskyttelse af fysiske personers rettigheder og frihedsrettigheder.

Kravet om, at den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau, der passer til risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, giver anledning til overvejelse om, hvorledes den dataansvarlige kan gribe denne opgave an.

Som udgangspunkt er det den dataansvarlige, som beslutter den nærmere fremgangsmåde og systematik. Det er nærliggende, at de følgende, vejledende fire trin vil kunne indgå i den dataansvarliges overvejelser:

[575] Den fælles offentlige digitaliseringsstrategi for 2016-2020.
[576] Den internationale standardiseringsorganisation, International Organization for Standardization, ISO.

1. Identifikation og vurdering af risici
2. Identifikation af mulige foranstaltninger
3. Gennemgang af, hvilke foranstaltninger som imødegår relevante risici, så et passende sikkerhedsniveau opnås.
4. Implementering af de foranstaltninger som det besluttes at gennemføre.

Ad trin 1:

I dette trin har den dataansvarlige fordel af sit kendskab til, hvorledes behandlingen af personoplysninger sker, hvilke midler der aktuelt anvendes ved behandlingen, samt den konkrete kontekst som behandlingen forgår i. Med dette som udgangspunkt kan den dataansvarlige søge at identificere, hvilke risici behandlingen udgør for fysiske personers rettigheder og frihedsrettigheder.

Når risikobilledet udfoldes, kan der f.eks. søges vejledning i anneks B i den ovenfor nævnte standard ISO/IEC DIS 29134 *Information technology -- Security techniques -- Privacy impact assessment – Guidelines*. Her findes mange eksempler på risici og trusler, som det formentlig vil være relevant at overveje og tage stilling til, også for så vidt angår risikoanalyser.

Hvis der f.eks. anvendes Cloud Computing, kan der tillige findes vejledning i publikationen *Cloud Computing Risk Assessment*[577] fra ENISA[578]. Artikel 29-gruppen har også udgivet en række udtalelser, som kan bruges vejledende, idet de bl.a. adresserer risici i forbindelse med nyere teknologier som f.eks. Cloud Computing, Internet of Things, biometri, ansigtsgenkendelse og geolokalisering i forbindelse med smarte mobile enheder. Herudover har Datatilsynet, som også tidligere nævnt, på tilsynets hjemmeside publiceret en række vejledninger i form af de såkaldte IT-sikkerhedstekster, som tematiseret udfolder og belyser risici forbundet med behandling af personoplysninger.

Efter at have udfoldet de risici, som er aktuelle, kan den dataansvarlige foretage en vurdering af de aktuelle risici med henblik på at tage stilling til, hvilke risici der skal træffes foranstaltninger til imødegåelse af, for at opnå et passende sikkerhedsniveau.

Ad trin 2:

Efter at have identificeret de risici, der skal imødegås ved foranstaltninger for, at et passende sikkerhedsniveau kan etableres, står den dataansvarlige overfor at skulle tage stilling

[577] https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
[578] The European Union Agency for Network and Information Security (ENISA).

til, hvilke foranstaltninger der i den aktuelle situation kan være relevante. Også i dette trin har den dataansvarlige fordel af sit kendskab til, hvorledes behandlingen af personoplysninger sker, hvilke midler der aktuelt anvendes ved behandlingen, samt den konkrete kontekst som behandlingen forgår i. Hvilke foranstaltninger, der vil være mest hensigtsmæssige, afhænger af de konkrete aktuelle omstændighederne og situationen ved den aktuelle behandling.

Ved identifikation af, hvilke foranstaltninger det kan være relevant at gennemføre, kan der f.eks. søges vejledning i ISO 27001-standardens anneks A, som indeholder en omfattende liste af kontrolmål og kontroller. Disse kontrolmål og kontroller modsvarer foranstaltninger, der kan træffes.

Ved udfoldelse af mulighederne for at træffe foranstaltninger, kan andre skriftsteder også være relevante at inddrage, alt afhængig af omstændighederne og situationen ved den aktuelle behandling. I denne forbindelse kan der igen peges på muligheden for at søge vejledning i publicerede udtalelser fra Artikel 29-gruppen og Datatilsynets IT-sikkerhedstekster. Endvidere kan der peges på publikationer fra Center fra Cybersikkerhed og Digitaliseringsstyrelsen, f.eks. *Cyberforsvar der virker*.[579]

Ad trin 3:

Sammenhængen mellem reelle risici og foranstaltninger er yderst sjældent en-til-en. I praksis imødegås en identificeret risiko ved kombination af forskellige foranstaltninger, som komplementerer hinanden og tilsammen reducerer den identificerede risiko, så et passende sikkerhedsniveau opnås.

Hvilken kombination af foranstaltninger det vil være relevant for den dataansvarlige at tage i betragtning afhænger, foruden af risikoen: (i) af hvorledes behandlingen af personoplysninger aktuelt foregår, (ii) af de midler der aktuelt anvendes ved behandlingen, samt (iii) af den konkrete kontekst som behandlingen forgår i. Når det overvejes, hvilke kombinationer af foranstaltninger, der kan imødegå en risiko, kan det være hensigtsmæssig at have øje for enkle grundprincipper, såsom isolation, adskillelse og forsvar i dybden.[580]

Når de, henset til risikoen, relevante mulige foranstaltninger er kortlagt, har den dataansvarlige et grundlag for at beslutte, hvilke foranstaltninger som aktuelt skal gennemføres, så der opnås et passende sikkerhedsniveau.

[579] https://fe-ddis.dk/cfcs/CFCSDocuments/Cyberforsvar%20der%20virker.pdf
[580] https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/vedroerende-uvedkommendes-adgang-til-personoplysninger-rigspolitiets-jnr-2013-079-76/

Ad trin 4:

I dette trin træffer den dataansvarlige beslutning om, hvilke foranstaltninger, som skal gennemføres for at sikre et sikkerhedsniveau, der passer til risiciene for fysiske personers rettigheder og frihedsrettigheder.

Ad trin 1-4:

Overvejelser om behandlingssikkerhed og foranstaltninger er endvidere noget, som den dataansvarlige bør gøre med regelmæssige mellemrum for at kunne imødegå ændringer i risikobilledet som følge af bl.a. tekniske og organisatoriske forandringer hos den dataansvarlige selv (og eventuelle databehandlere), samt ændrede trusler fra omverdenen og internt i den dataansvarliges organisation, samt hos eventuelle databehandlere.

Ved design og udvikling af nye løsninger til behandling af personoplysninger og/eller ved større ændringer i eksisterende løsninger, vil det også være muligt at indarbejde fremgangsmåden, der er beskrevet i de fire ovenstående punkter. Ved at gøre det, vil behandlingssikkerhed og foranstaltninger kunne indarbejdes i løsningens organisatoriske og tekniske udformning og implementering. Fordelen ved dette er, at mulighederne for at finde passende foranstaltninger ikke begrænses af allerede implementerede designbeslutninger, som måske er gjort uden tilstrækkelig øje for behandlingssikkerhed.

I forbindelse med etablering af nye behandlinger, eller ved væsentlige ændringer i en eksisterende behandling, kan den dataansvarlige stå overfor at skulle gennemføre en konsekvensanalyse. Det vil i forbindelse med en konsekvensanalyse være muligt at indarbejde fremgangsmåden, der er beskrevet i de fire ovenstående trin. Herved vil den dataansvarlige på et tidligt tidspunkt i processen kunne indarbejde behandlingssikkerhed og målrette konsekvensanalysen mod opfyldelse af artikel 32.

Det bemærkes, at en konsekvensanalyse – i henhold til forordningens artikel 35 – er mere vidtgående og omfangsrig end de fire ovenstående trin.

I forbindelse med konsekvensanalyser kan der peges på, at artikel 39 om databeskyttelsesrådgiverens opgaver i stk. 1, litra c, åbner mulighed for, at den dataansvarlige kan anmode databeskyttelsesrådgiveren om at rådgive med hensyn til konsekvensanalysen vedrørende databeskyttelse.

Afslutningsvis bemærkes, at forordningens artikel 32, stk. 3, er udtryk for en nyskabelse. Forordningens artikel 32, stk. 4, svarer derimod til persondatalovens § 41, stk. 1, og er således i al væsentlighed en videreførelse af det, der gælder efter persondataloven.

5.11. Anmeldelse af brud på sikkerheden, artikel 33

5.11.1. Præsentation

Der følger ikke en generel forpligtelse om at anmelde brud på persondatasikkerheden til Datatilsynet efter databeskyttelsesdirektivet eller persondataloven. Derimod har der siden 2011 i forhold til telesektoren og virksomheder, som er omfattet af den særlige telelovgivning, været en lovgivningsmæssig forpligtelse til at anmelde brud på persondatasikkerheden til Erhvervsstyrelsen.

Databeskyttelsesforordningen lægger – i modsætning hertil – op til en ordning i artikel 33, hvorefter der generelt i forhold til alle dataansvarlige som udgangspunkt vil komme til at gælde en forpligtelse om at anmelde brud på persondatasikkerheden til tilsynsmyndigheden.

5.11.2. Gældende ret

Virksomheder eller offentlige myndigheder, der har sikkerhedsbrud i forbindelse med behandling af personoplysninger, har generelt ikke pligt til at underrette tilsynsmyndigheden om bruddet. Persondataloven indeholder således f.eks. ikke bestemmelser, der pålægger dataansvarlige at anmelde brud på persondatasikkerheden til Datatilsynet.

Telesektoren og virksomheder, som er omfattet af den særlige telelovgivning, har imidlertid siden 2011 – som en undtagelse til det generelle udgangspunkt – været underlagt en pligt til at underrette Erhvervsstyrelsen om brud på persondatasikkerheden, jf. § 8 i lov om elektroniske kommunikationsnet og -tjenester[581] og den i henhold bl.a. hertil udstedte bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.[582] Der er tale om regler, der gennemfører dele af bl.a. Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om databeskyttelse inden for elektronisk kommunikation, som ændret ved Europa-Parlamentets og

[581] Lovbekendtgørelse nr. 128 af 7. februar 2014, som ændret ved lov nr. 1567 af 15. december 2015.
[582] Der kan i den forbindelse henvises til Erhvervsstyrelsens vejledning til bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

Rådets direktiv 2009/136/EF af 25. november 2009 (e-databeskyttelsesdirektivet) i dansk ret.[583]

Bekendtgørelsen finder ifølge § 1 anvendelse på styring af risici for persondatasikkerhed og underretning om brud på persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

Ved begrebet "brud på persondatasikkerheden" skal ifølge bekendtgørelsens § 2 forstås sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles i forbindelse med udbuddet af en offentlig elektronisk kommunikationstjeneste.

Af bekendtgørelsens § 5, stk. 1, fremgår, at underretning om brud på persondatasikkerheden skal ske til Erhvervsstyrelsen og i overensstemmelse med artikel 2 i Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden.

Af forordningen om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerhedens artikel 2, stk. 1, fremgår, at udbyderen skal underrette den kompetente nationale myndighed om samtlige brud på persondatasikkerheden.

Udbyderen skal ifølge forordningen om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerhedens artikel 2, stk. 2, 1. afsnit, underrette den kompetente nationale myndighed om bruddet på persondatabeskyttelsen senest 24 timer efter, at bruddet er påvist, når dette er praktisk muligt. Udbyderen skal i sin underretning af den kompetente nationale myndighed vedlægge de oplysninger, der er angivet i bilag I til forordningen, jf. artikel 2, stk. 2, 2. afsnit.

Et brud på persondatasikkerheden skal ifølge forordningen om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerhedens artikel 2, stk. 2, 3. afsnit, i øvrigt anses for at være påvist, hvis en udbyder har opnået tilstrækkelig kendskab til, at en sikkerhedshændelse er indtruffet, og at den har kompromitteret persondatasikkerheden, således at der kan afgives en hensigtsmæssig underretning som krævet ifølge denne forordning. Efter forordningens præambelbetragtning nr. 8 vil en simpel formodning for, at et brud på persondatasikkerheden har fundet sted, eller en simpel påvisning af en hændelse ikke være tilstrækkeligt, til at anse et brud på persondatasikkerheden for at være påvist i

[583] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om databeskyttelse inden for elektronisk kommunikation (EF-Tidende 2002, nr. L 201, s. 37), og Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (EF-Tidende 2009, nr. L 337, s. 11) (e-databeskyttelsesdirektivet).

forordningens forstand. Bruddet er således ikke påvist, hvis de oplysninger, der er til rådighed for udbyderen, er utilstrækkelige til at fastslå dette, selvom udbyderen gør sit bedste for at skabe afklaring.

Det følger af forordningen om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerhedens artikel 2, stk. 3, 1. afsnit, at udbyderen må foretage en *indledende underretning* af den kompetente nationale myndighed senest 24 timer efter påvisning af bruddet på persondatabeskyttelsen, hvis alle de i bilag I angivne oplysninger ikke foreligger, og der er behov for yderligere efterforskning af bruddet på persondatasikkerheden. Denne indledende underretning af den kompetente nationale myndighed skal indeholde de oplysninger, der er anført i bilag I, afdeling 1.[584]

Udbyderen skal herefter foretage en *anden underretning* af den kompetente nationale myndighed så hurtigt som muligt og senest tre dage efter den indledende underretning. Denne anden underretning skal indeholde de oplysninger, der er anført i bilag I, afdeling 2,[585] og om nødvendigt ajourføre de oplysninger, der allerede er afgivet.

Hvis udbyderen på trods af sin efterforskning ikke er i stand til at forelægge alle oplysninger senest tre dage efter den indledende underretning, skal udbyderen ifølge forordningen om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerhedens artikel 2, stk. 3, 2. afsnit, afgive alle disponible oplysninger inden for denne tidsfrist og forelægge den kompetente nationale myndighed en begrundelse for den forsinkede underretning om de resterende oplysninger.

---

[584] Oplysninger om *udbyderens identitet* i form af udbyderens navn (1), identitet og kontaktoplysninger for den databeskyttelsesansvarlige eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes (2), hvorvidt det drejer sig om den første eller anden underretning (3), og en række *indledende oplysninger om bruddet på persondatasikkerheden (suppleres i senere underretninger, hvis det er relevant)* i form af dato og tidspunkt for hændelsen (hvis dette er kendt; om nødvendigt kan der gives et skøn) og for påvisningen af hændelsen (4), omstændighederne ved bruddet på persondatasikkerheden (f.eks. bortkomst, tyveri, kopiering) (5), karakter og indhold af de berørte personoplysninger (6), tekniske og organisatoriske foranstaltninger, som udbyderen anvender (eller vil anvende), i henseende til de berørte personoplysninger (7) og relevant anvendelse af andre udbydere (eventuelt) (8).

[585] *Yderligere oplysninger om bruddet på persondatasikkerheden* i form af resumé af den hændelse, der forårsagede bruddet på persondatasikkerheden (herunder det fysiske sted, hvor bruddet fandt sted, og hvilket lagringsmedie der blev berørt heraf) (9), antal berørte abonnenter eller fysiske personer (10), potentielle konsekvenser og potentielle krænkelser af abonnenter eller fysiske personer (11), tekniske og organisatoriske foranstaltninger, som udbyderen har sat i værk for at afhjælpe potentielle krænkelser (12) *og eventuel yderligere underretning af abonnenter eller fysiske personer* og i så fald underretningens indhold (13), anvendte kommunikationsmidler (14), antal underrettede abonnenter eller fysiske personer (15) samt i tilfælde af *eventuelle tværnationale spørgsmål* da oplysninger om brud på persondatasikkerheden, som involverer abonnenter eller fysiske personer i andre medlemsstater (16) og underretning af andre kompetente nationale myndigheder (17).

Udbyderen forelægger hurtigst muligt de resterende oplysninger for den kompetente nationale myndighed og ajourfører om nødvendigt de oplysninger, der allerede er afgivet.

Ifølge forordningen om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerhedens artikel 2, stk. 4, stiller den kompetente nationale myndighed i øvrigt sikre elektroniske midler til rådighed, således at alle udbydere, der er etableret i den pågældende medlemsstat, kan underrette om brud på persondatasikkerheden, tillige med oplysninger om procedurerne for adgang og brug af denne.[586] I Danmark er dette krav implementeret ved, at udbydere af elektroniske kommunikationstjenester via portalen Virk, hvor virksomhederne allerede foretager deres øvrige indberetninger, kan indberette brud på persondatasikkerheden til Erhvervsstyrelsen.[587]

Det følger endvidere af forordningens artikel 2, stk. 4, at når bruddet på persondatasikkerheden krænker abonnenter eller fysiske personer fra andre medlemsstater end den kompetente nationale myndigheds medlemsstat, hvori der er underrettet om bruddet på persondatasikkerheden, informerer den kompetente nationale myndighed de øvrige berørte nationale myndigheder. For at lette anvendelsen af denne bestemmelse opretter og ajourfører Kommissionen en liste over de kompetente nationale myndigheder og de relevante kontaktpunkter.

Udbydere af offentlige elektroniske kommunikationstjenester skal endvidere ifølge § 6 i bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester føre optegnelser over brud på persondatasikkerheden. Optegnelserne skal indeholde oplysninger om omstændighederne vedrørende bruddene, deres virkninger og de afhjælpende foranstaltninger, der er truffet. Optegnelserne skal være tilstrækkeligt detaljerede til, at Erhvervsstyrelsen kan føre kontrol med overholdelsen af Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013, jf. bekendtgørelsens § 8. Optegnelserne skal kun indeholde de oplysninger, der er nødvendige til dette formål.

Det bemærkes, at Kommissionen den 10. januar 2017 har fremsat et forslag til Europa-Parlamentets og Rådets forordning om respekten for privatlivet og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om privatlivets fred og elektronisk kommunikation) (KOM/2017/010 endelig).

---

[587] Se i den forbindelse også Erhvervsstyrelsens hjemmeside, hvorfra der via et link til virk.dk kan foretages elektronisk underretning om brud på persondatasikkerheden til styrelsen.

Formålet med forslaget er dels at opdatere de gældende regler på området og udvide anvendelsesområdet til alle udbydere af elektronisk kommunikation og dels at skabe nye muligheder for at behandle datakommunikation og styrke tilliden til og sikkerheden i det digitale indre marked. Samtidig tilpasses reglerne for elektronisk kommunikation med databeskyttelsesforordningen. Det er meningen, at forslaget skal vedtages senest den 25. maj 2018, så det kan finde anvendelse samtidig med, at databeskyttelsesforordningen finder anvendelse.

Forordningsforslaget lægger med sin nuværende ordlyd bl.a. op til, at forpligtelsen til at anmelde brud på persondatasikkerheden fremover alene vil komme til at gælde, hvis dette følger af bestemmelserne i databeskyttelsesforordningen. Det fremgår i øvrigt generelt af forslagets artikel 1, at den generelle databeskyttelsesforordning vil finde anvendelse på behandling af personoplysninger i forbindelse med elektronisk kommunikation i det omfang, der er tale om et databeskyttelsesretligt spørgsmål, som ikke er reguleret i dette forordningsforslag. Forordningsforslagets regler om behandling af personoplysninger vil med andre ord være at anse for såkaldte sektorspecifikke databeskyttelsesregler, der på sigt, når reglerne er blevet endelig vedtaget og finder anvendelse, vil specificere og supplere de generelle regler om beskyttelse af personoplysninger i databeskyttelsesforordningen i forhold til de dataansvarlige i den elektroniske kommunikationssektor, der falder ind under disse regler.

Endvidere fremgår det af forslagets kapitel IV, at opgaven med at føre tilsyn med og håndhæve forordningens regler skal placeres hos de tilsynsmyndigheder, der har ansvaret med at føre tilsyn med og håndhæve databeskyttelsesforordningen (forslagets artikel 18). Der lægges endvidere op til at udvide Det Europæiske Databeskyttelsesråds ansvars- og kompetenceområde til også at gælde dette område (forslagets artikel 19), ligesom de særlige regler, der findes i databeskyttelsesforordningens kapitel VI og VII om one-stop-shop mekanismen og sammenhængsmekanisme også vil finde anvendelse i forbindelse med grænseoverskridende spørgsmål vedrørende denne forordning (artikel 20). Bøde- og sanktionsniveauet for overtrædelse af forordningen vil ifølge forslaget være de samme som i databeskyttelsesforordningen.

5.11.3. Databeskyttelsesforordningen

5.11.3.1. Databeskyttelsesforordningens artikel 33, stk. 1

Det følger af forordningens artikel 33, stk. 1, at der ved brud på persondatasikkerheden anmelder den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, bruddet på persondatasikkerheden til den tilsynsmyndighed, som er kompetent i overensstemmelse med artikel 55, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettig-

heder eller frihedsrettigheder. Foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.

Bestemmelsen tager sigte på at tilvejebringe transparens og især på at sikre, at den dataansvarlige reagerer, når der opstår et sikkerhedsbrud. Den dataansvarlige skal have indrettet sine procedurer således, at en sådan meddelelse kan gives, jf. nedenfor ad artikel 33, stk. 3, om, hvad der skal meddeles.[588]

Ved begrebet *brud på persondatasikkerhed* forstås ifølge forordningens artikel 4, nr. 12, et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Et brud på persondatasikkerheden kan f.eks. rent teknisk ske, når den dataansvarliges IT-systemer med personoplysninger ikke er tilstrækkelig sikret, således at udefrakommende får adgang til oplysningerne (f.eks. hacking). Det kan imidlertid også være den dataansvarliges egen håndtering af personoplysningerne, der kan forårsage et brud, f.eks. hvis den dataansvarlige ubeføjet videregiver eller ændrer personoplysningerne eller ulovligt eller hændeligt (f.eks. brand eller oversvømmelse) tilintetgør personoplysningerne.

Som eksempler på brud på persondatasikkerheden kan nævnes:

1) Andre personer end den eller de personer hos dataansvarlige, der er autoriseret til det, får (uautoriseret) adgang til personoplysninger. Det kan både være personer uden for eller inden for dataansvarliges organisation.
2) Den dataansvarliges medarbejdere ændrer eller sletter persondata ved et uheld.
3) Brud på den dataansvarliges server, hvor uvedkommende har fået indsigt i personoplysninger – f.eks. kundedatabasens CPR-oplysninger, kreditkort-oplysninger el.lign.
4) Den dataansvarliges medarbejdere videregiver ubevidst eller bevidst personoplysninger om en borger/kunde til en anden borger/kunde – eller måske ligefrem flere andre uvedkommende personer.
5) Når manglede kryptering af den dataansvarliges hjemmeside indeholdende f.eks. et kundelogin resulterer i, at en eller flere uvedkommende får direkte adgang til kundens personoplysninger.

[588] Peter Blume, Den nye persondataret (2016), s. 122.

I forordningens præambelbetragtning nr. 85 gives endvidere eksempler på, hvilke konsekvenser brud på persondatasikkerheden kan have for fysiske personer. Det fremgår således af præambelbetragtningen, at et brud på persondatasikkerheden kan, hvis det ikke håndteres på en passende og rettidig måde, påføre fysiske personer fysisk, materiel eller immateriel skade, såsom tab af kontrol over deres personoplysninger eller begrænsning af deres rettigheder, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, uautoriseret ophævelse af pseudonymisering, skade på omdømme, tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt, eller andre betydelige økonomiske eller sociale konsekvenser for den berørte fysiske person.

Som det fremgår af bestemmelsens ordlyd, aktiveres den dataansvarliges forpligtelse til at foretage anmeldelse af brud på persondatasikkerhed til tilsynsmyndigheden, efter at den *dataansvarlige er blevet bekendt med, at der er sket et brud på persondatasikkerheden.* En simpel formodning om, at et brud på persondatasikkerheden har fundet sted, eller en simpel påvisning af en hændelse vurderes i den forbindelse ikke at være tilstrækkeligt til at anse et brud på persondatasikkerheden for at være "sket" i forordningens forstand. En sådan simpel formodning kan dog bevirke, at den dataansvarlige skal overveje behandlingssikkerheden, jf. forordningens artikel 32.

I vurderingen af, om et brud er "sket", må der antages at skulle tages særligt hensyn til, om de oplysninger, der er nævnt i forordningens artikel 33, stk. 3, står til rådighed for udbyderen.

Der kan i den forbindelse også henvises til den ovenfor omtalte Kommissions-forordning (EU) nr. 611/2013 af 24. juni 2013, hvor det af forordningens artikel 2, stk. 2, 3. afsnit, fremgår, at et brud på persondatasikkerheden skal anses for at være påvist, hvis en udbyder har opnået tilstrækkelig kendskab til, at en sikkerhedshændelse er indtruffet, og at den har kompromitteret persondatasikkerheden, således at der kan afgives en hensigtsmæssig underretning som krævet ifølge denne forordning.

Som det imidlertid samtidig er anført nedenfor ad forordningens artikel 33, stk. 4, som tillader den dataansvarlige at sende de i stk. 3 nævnte oplysninger til tilsynsmyndigheden trinvis, så må det dermed ligeledes antages, at selv om den dataansvarlige ikke er i stand til at afgive alle de i stk. 3 listede oplysninger samlet inden for 72 timer, kan dette ikke udgøre en begrundelse for at have undladt at efterleve det overordnede krav i forordningens artikel 33, stk. 1, om at anmeldelse af bruddet på persondatasikkerheden skal ske til tilsynsmyndigheden inden for 72 timer.

For så vidt angår de tilfælde, hvor den dataansvarlige har overladt behandlingen af personoplysninger til en databehandler, henvises til forordningens artikel 33, stk. 2, der er nærmere omtalt nedenfor.

Det fremgår endvidere af forordningens artikel 33, stk. 1's ordlyd, at den dataansvarliges anmeldelse af brud på persondatasikkerheden som hovedregel skal ske *uden unødig forsinkelse*. Heri ligger, at den dataansvarlige er forpligtet til at underrette tilsynsmyndigheden om sikkerhedsbruddet, så snart det er muligt – også, hvis dette tidspunkt indtræder, før udløbet af de 72 timer. Tidsgrænsen på de 72 timer skal med andre ord ikke forstås således, at den dataansvarlig kan vente med at anmelde et brud på persondatasikkerheden, indtil/lige før fristen udløber, hvis den dataansvarlige er i stand hertil på et tidligere tidspunkt.

Vedrørende kravet om en anmeldelse af et brud på persondatasikkerheden uden unødig forsinkelse fremgår i øvrigt bl.a. af præambelbetragtning nr. 87, at om anmeldelsen fandt sted uden unødig forsinkelse bør fastslås, under særlig hensyntagen til karakteren og alvoren af bruddet på persondatasikkerheden og dets konsekvenser og skadevirkninger for den registrerede.

Med mindre tilsynsmyndigheden er utilgængelig for enhver form for kontakt, er det svært at forestille sig situationer, der gør det umuligt for en dataansvarlig at foretage en anmeldelse til tilsynsmyndigheden inden for de 72 timer. Naturkatastrofer eller andet, der f.eks. afbryder elektroniske kommunikationsforbindelser kan være en hindring, men den dataansvarlige kan i sådanne tilfælde ikke se bort fra muligheden for fysisk forsendelse/overdragelse af anmeldelsen, f.eks. via postvæsnet eller kurerservice, når den dataansvarlige skal efterleve kravet om, at anmeldelse af brud på persondatasikkerhed skal ske til tilsynsmyndigheden uden unødvendig forsinkelse.

Tidsgrænsen på de 72 timer for anmeldelsen af brud på persondatasikkerhed til tilsynsmyndigheden, er ifølge bestemmelsen imidlertid ikke ubetinget, men foretages anmeldelsen til tilsynsmyndigheden ikke inden for de 72 timer, skal anmeldelsen ledsages af en begrundelse for forsinkelsen. Overskrides de 72 timer, skal det således være fordi, det – af særlige grunde, som den dataansvarlige er i stand til at redegøre nærmere for – ikke var muligt for den dataansvarlige at foretage anmeldelsen inden fristens udløb.

Der henvises i den forbindelse også til det nedenfor anførte om databeskyttelsesforordningens artikel 33, stk. 4, om den dataansvarliges mulighed for at meddele de oplysninger, der ifølge forordningens artikel 33, stk. 3, skal ledsage anmeldelsen trinvist til tilsynsmyndigheden.

Forordningens artikel 33, stk. 1, rummer endvidere mulighed for, at den dataansvarlige efter en nærmere vurdering af bruddet på persondatasikkerhed helt kan undlade at foretage anmeldelse, hvis det er *usandsynligt*, at bruddet på persondatasikkerheden indebærer en *risiko* for fysiske personers rettigheder eller frihedsrettigheder. Der må være en rimelig høj grad af sikkerhed herfor. For nærmere om "fysiske personers rettigheder eller frihedsrettigheder" henvises til afsnit 5.12. om artikel 34.

Hvis det efter artikel 34 vurderes, at et sikkerhedsbrud indebærer en høj risiko for fysiske personers rettigheder og frihedsrettigheder, så der skal ske underretning af den registrerede, så vil sikkerhedsbruddet også medføre, at bruddet indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder, og der vil også skulle ske anmeldelse til tilsynsmyndigheden efter artikel 33. For nærmere om underretningspligten efter artikel 34 se afsnit 5.12. Der vil dog også være situationer, hvor der skal ske anmeldelse til tilsynsmyndigheden i tilfælde, hvor der ikke er en underretningspligt efter artikel 34.

Der kunne f.eks. være tale om en situation, hvor en dataansvarlig har mistet et bærbart medie, hvorpå der er lagret persondata i krypteret form. Der kan være anvendt en tilstrækkelig stærk kryptering, som ikke kan brydes eller omgås inden for en tilstrækkelig lang årrække, og uvedkommende har ikke og får ikke mulighed for at dekryptere data på normal vis – f.eks. ved at komme i besiddelse af rette krypteringsnøgle. Den dataansvarlige kan i så fald siges at have en formodning om, at persondata er beskyttet på en sådan måde, at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Bevisbyrden for, at data virkelig var beskyttet tilstrækkeligt, påhviler den dataansvarlige.[589] Dette kan blive aktuelt senere, f.eks. i forbindelse med en sag hos tilsynsmyndigheden, hvor den dataansvarlige således skal være i stand til at begrunde, hvorfor anmeldelse af bruddet på persondatasikkerheden til tilsynsmyndigheden blev fravalgt.

Anmeldelse i overensstemmelse med forordningens artikel 33, vil kunne resultere i, at en dataansvarlig bliver udsat for tilsyn fra tilsynsmyndighedens side og i sidste ende idømmes en sanktion efter forordningen, hvorfor det kan overvejes, hvorvidt anmeldelsespligten efter artikel 33 er i strid med forbuddet mod selvinkriminering.

Det følger af retssikkerhedslovens § 1, stk. 3, at lovens kapitel 4 finder anvendelse i tilfælde, hvor der i lovgivningen mv. er fastsat pligt til at meddele oplysninger til den offentlige forvaltning. I kapitlet fastsættes regler for, i hvilket omfang regler i lovgivningen mv. om

[589] I databeskyttelsesforordningens præambeltragtning 85 omtales denne situation på følgende måde: "medmindre den dataansvarlige i overensstemmelse med ansvarlighedsprincippet kan påvise".

pligt til at meddele oplysninger til den offentlige forvaltning gælder, når en person er mistænkt for at have begået et strafbart forhold.[590]

Det fremgår således af retssikkerhedslovens § 10, at hvis der er konkret mistanke om, at en enkeltperson eller juridisk person har begået en lovovertrædelse, der kan medføre straf, gælder bestemmelser i lovgivning mv. om pligt til at meddele oplysninger til myndigheden ikke i forhold til den mistænkte, medmindre det kan udelukkes, at de oplysninger, der søges tilvejebragt, kan have betydning for bedømmelsen af den formodede lovovertrædelse. Det fremgår af Retssikkerhedskommissionens betænkning nr. 1428, at bestemmelsen bl.a. skal ses i sammenhæng med den praksis, som knytter sig til artikel 6, stk. 1, i Den Europæiske Menneskerettighedskonvention, hvorefter en person, som er anklaget for en forbrydelse, har ret til ikke at udtale sig om den påståede forbrydelse, og til ikke at blive tvunget til at medvirke til at opklare den påståede forbrydelse.[591]

Det er en grundlæggende betingelse for anvendelse af beskyttelsen mod selvinkriminering, at den europæiske menneskerettighedskonventions artikel 6 finder anvendelse på det tidspunkt, hvor en person er sigtet i artikel 6's forstand. Beskyttelsen efter artikel 6 gælder derfor fra det tidspunkt, hvor den pågældende er sigtet for en strafferetlig overtrædelse i den europæiske menneskerettighedskonventions forstand, hvilket normalt fortolkes enten som en officiel notifikation/sigtelse om strafbart forhold eller en mere konkret vurdering af, at den pågældende reelt er genstand for en strafferetlig efterforskning.[592]

Den Europæiske Menneskerettighedsdomstol udtalte endvidere i sagen Allen v. The United Kingdom af 10. september 2002, at pligt til at indgive selvangivelse til skattemyndighederne under trussel om bøde dog ikke i sig selv er i strid med selvinkrimineringsforbuddet. Domstolen lagde bl.a. vægt på, at pligt til at indgive selvangivelse til skattemyndighederne er en del af skattesystemet, og at det ville være vanskeligt at have et effektivt skattesystem uden denne pligt.

Domstolen lagde endvidere vægt på, at de oplysninger, som klager gav til myndighederne, ikke blev anvendt til at inkriminere klager for et strafbart forhold begået før det tidspunkt, hvor klager gav oplysningerne. Domstolen lagde ligeledes vægt på, at klager ikke var blevet tiltalt for ikke at have leveret oplysninger, der kunne inkriminere klager i en verserende eller en påtænkt straffesag. Afgørelsen i Allen-sagen understreger således, at strafsanktio-

[590] Retssikkerhedskommissionens betænkning 1428/2003, s. 194.
[591] Retssikkerhedskommissionens betænkning 1428/2003 s. 194.
[592] Deweer 27/2 1990, præmis 42 og 46 samt Eckle 17/7 1987, præmis 73, jf. Peer Lorenzen, Jonas Christoffersen, Nina Holst-Christensen, Peter Vedel Kessing, Sten Schaumburg-Müller og Jens Vedsted-Hansen, Den Europæiske Menneskerettighedskonvention med kommentarer, 3. udgave (2011), s 438.

nerede oplysningspligter ikke må anvendes til at tvinge en person til at afgive forklaring mv. om en allerede begået forbrydelse, som den pågældende er anklaget for at have begået, men at anvendelse af en strafsanktioneret oplysningspligt ikke i sig selv er i strid med selvinkrimineringsforbudet.[593]

Når en dataansvarlig anmelder brud på persondatasikkerheden til tilsynsmyndigheden efter artikel 33, vil dette ske umiddelbart efter, at den dataansvarlige er blevet bekendt med, at der er sket et brud på persondatasikkerheden. Den dataansvarlige vil derfor ikke være sigtet eller mistænkt for overtrædelse af databeskyttelsesforordningen, hvorfor anmeldelsen ikke er i strid med forbuddet mod selvinkriminering efter retssikkerhedslovens § 10 og den europæiske menneskerettighedskonventions artikel 6. Dette støttes også af, at EU-lovgiver har vurderet, at den dataansvarlige skal have denne anmeldelsespligt (som bl.a. også må antages at være af hensyn til en velfungerende beskyttelse af datasikkerheden), hvilket også taler for, at anmeldelse efter artikel 33 ikke er i strid med selvinkrimineringsforbuddet.

På en række områder har borgere og virksomheder pligt til løbende at indberette visse oplysninger til en myndighed. Så længe der ikke består en mistanke, finder retssikkerhedslovens § 10 og den europæiske menneskerettighedskonventions artikel 6 ikke anvendelse. Myndigheden vil således stadig kunne anvende oplysningspligten over bl.a. den mistænkte borger eller virksomhed, i det omfang det kan udelukkes, at de oplysninger, som den fortsatte løbende pligt til at foretage indberetning vedrører, vil have betydning for det eller de forhold, som den foreliggende mistanke omfatter.[594]

I en besvarelse til Retsudvalget anføres det endvidere, at det faktum, at der måtte være konkret mistanke om, at reglerne er overtrådt i en bestemt periode eller med hensyn til konkrete forhold, således ikke er ensbetydende med, at der vil være konkret mistanke om, at reglerne (også) vil bliver overtrådt i senere perioder mv.[595]

5.11.3.2. Databeskyttelsesforordningens artikel 33, stk. 2

Forordningens artikel 33, stk. 2, pålægger eventuel(le) databehandler(e), efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden, uden unødig forsinkelse at underrette den dataansvarlige herom.

[593] Retssikkerhedskommissionens betænkning 1428/2003, afsnit 3.6.
[594] Ole Hasselgaard, Jens Møller og Jørgen Steen Sørensen, Retssikkerhedsloven med kommentarer, (2005), side 183-184.
[595] Ole Hasselgaard, Jens Møller og Jørgen Steen Sørensen, Retssikkerhedsloven med kommentarer, (2005), side 184.

Der er tale om en absolut regel, som databehandleren skal efterleve i alle tilfælde. Bestemmelsen åbner f.eks. ikke mulighed for, at databehandleren undlader at underrette den dataansvarlige om et brud på persondatasikkerheden med henvisning til, at databehandleren selv har vurderet, at det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

5.11.3.3. Databeskyttelsesforordningens artikel 33, stk. 3

Det følger af forordningens artikel 33, stk. 3, at den dataansvarliges anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden efter stk. 1, *mindst* skal indeholde den information, der opregnes i artikel 33, stk. 3, litra a-d. Der er med andre ord ikke tale om en udtømmende liste over indholdet af informationer, og litra a-d udelukker dermed ikke, at der skal afgives yderligere informationer for at sikre efterlevelse af artikel 33, stk. 1.

Det fremgår af forordningens artikel 33, stk. 3, *litra a,* at anmeldelsen skal beskrive karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af person-oplysninger. Det er ikke ganske klart, hvad der med menes med "registreringer", men brugen af denne betegnelse indicerer, at meddelelsen ikke direkte skal specificere, hvilke personoplysninger som er berørt.[596]

Af *litra b* i forordningens artikel 33, stk. 3, fremgår det, at anmeldelsen endvidere skal angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes. Reglen sikrer, at tilsynsmyndigheden har ét kontaktpunkt, hvorfra yderligere oplysninger kan indhentes i forbindelse med tilsynsmyndighedens behandling af bruddet på persondatasikkerheden. Hvis tilsynsmyndigheden fremsætter ønske om yderligere oplysninger, vil det være op til databeskyttelsesrådgiveren eller det eventuelle andet kontaktpunkt at tilvejebringe oplysningerne og viderebringe dem til tilsynsmyndigheden.

Herudover skal anmeldelsen ifølge forordningens artikel 33, stk. 3, *litra c*, beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden.

Det fremgår endelig af forordningens artikel 33, stk. 3, *litra d*, at anmeldelsen skal beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

[596] Peter Blume, Den nye persondataret (2016), s. 123.

Oplysningerne i litra a-d skal bidrage til, at tilsynsmyndigheden får mulighed for at følge og vurdere, at den dataansvarliges håndtering af bruddet på persondatasikkerheden sker på en adækvat måde. Tilsynsmyndigheden kan også anvende oplysningerne ved vurderingen af, hvorvidt der er behov for, at den intervenerer i henhold til forordningens artikel 34, stk. 4, eller gør brug af sine korrigerende beføjelser til midlertidigt eller definitivt at begrænse, herunder forbyde, behandling i henhold til forordningens artikel 58, stk. 2, litra f.

Det bemærkes, at hvor forordningens artikel 33, stk. 3, fastsætter krav til mindsteindholdet i en anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden, gælder der ingen nærmere formkrav til selve anmeldelsen. Forordningens artikel 33, stk. 3, indeholder heller ikke nærmere regler om, hvilke sprog der kan anvendes til anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden.

Når der fastsættes nærmere regler for, hvilket format og hvilke procedurer der skal anvendes ved anmeldelse af brud på persondatasikkerheden, bør der ifølge præambelbetragtning nr. 88 imidlertid tages hensyn til omstændighederne ved det pågældende brud, herunder om personoplysningerne var beskyttet med passende tekniske beskyttelsesforanstaltninger, der effektivt begrænser sandsynligheden for identitetssvig eller andre former for misbrug. Sådanne regler og procedurer bør endvidere tage hensyn til de retshåndhævende myndigheders legitime interesser, da en tidlig videregivelse unødigt kan hæmme undersøgelsen af omstændighederne ved et brud på persondatasikkerheden.

5.11.3.4. Databeskyttelsesforordningens artikel 33, stk. 4

Forordningens artikel 33, stk. 4, åbner mulighed for, at den dataansvarlige kan meddele oplysningerne omtalt i stk. 3 trinvist til tilsynsmyndigheden uden unødig yderligere forsinkelse, når og for så vidt som det ikke er muligt at give oplysningerne samlet. Dette må ses i lyset af, at de relevante oplysninger kan tage tid at afdække, og at delvise oplysninger i en situation med brud på persondatasikkerheden må formodes at være bedre for tilsynsmyndighedens handlemuligheder, end ingen information.

Det vil ikke være i overensstemmelse med bestemmelsen at tilbageholde relevante oplysninger med henblik på at give dem samlet til tilsynsmyndigheden, idet meddelelsen af oplysningerne skal ske *uden unødig yderligere forsinkelse*. Det må dermed ligeledes antages, at selv om den dataansvarlige ikke er i stand til at afgive alle de i stk. 3 listede oplysninger samlet inden for 72 timer, kan dette ikke udgøre en begrundelse for at have undladt at efterleve det overordnede krav i forordningens artikel 33, stk. 1, om at anmeldelse af bruddet på persondatasikkerheden skal ske til tilsynsmyndigheden inden for 72 timer.

5.11.3.5. Databeskyttelsesforordningens artikel 33, stk. 5
Ifølge forordningens artikel 33, stk. 5, skal den dataansvarlige dokumentere alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at artikel 33 er overholdt.

Tilsynsmyndigheden har ifølge bestemmelsen ikke forpligtelse til at indhente dokumentationen, men den dataansvarlige har pligt til at stille dokumentationen til rådighed for tilsynsmyndigheden, hvis myndigheden fremsætter ønske herom.

Da dokumentationen skal sætte tilsynsmyndigheden i stand til at kontrollere, at artikel 33 (og artikel 34 om underretning af den registrerede i tilfælde af et brud på persondatasikkerheden) er overholdt, må det antages, at dokumentationen skal indeholde de samme oplysninger, som er omtalt i artikel 33, stk. 3, men det vil f.eks. også være relevant, at den dataansvarlige bl.a. dokumenterer om, og i givet fald hvorledes, der er foretaget underretning om bruddet på persondatasikkerhed til den registrerede, som foreskrevet i artikel 34, stk. 1-3, fordi det har betydning for tilsynsmyndighedens eventuelle intervention i henhold til artikel 34, stk. 4.

5.11.3.6. Databeskyttelsesforordningens artikel 70, stk. 1, litra e, litra g og litra l
Af forordningens artikel 70, stk. 1, litra e, fremgår det i øvrigt, at Databeskyttelsesrådet på eget initiativ, efter anmodning fra et af sine medlemmer eller efter anmodning fra Kommissionen skal undersøge ethvert spørgsmål vedrørende anvendelsen af denne forordning og udstede retningslinjer, henstillinger og bedste praksis for at fremme ensartet anvendelse af denne forordning.

I forordningens artikel 70, stk. 1, litra f – m, opregnes herefter en række områder, hvor rådet skal udstede sådanne retningslinjer, henstillinger og bedste praksis i overensstemmelse med litra e. Et af de nævnte områder er: fastlæggelse af brud på persondatasikkerheden og den unødige forsinkelse omhandlet i artikel 33, stk. 1 og 2, og vedrørende de særlige omstændigheder, hvor en dataansvarlig eller en databehandler har pligt til at anmelde brud på persondatasikkerheden, jf. litra g.

De omhandlede retningslinjer mv. er ikke bindende for medlemsstaterne, men vil formentlig få en vis normerende effekt for de nationale tilsynsmyndigheder og må dermed antages at komme til at medvirke til at øge graden af harmonisering af udmøntningen af forordningens regler i medlems-staterne.

Endvidere fremgår det af forordningens artikel 70, stk. 1, litra l, at Databeskyttelsesrådet skal gennemgå den praktiske anvendelse af de retningslinjer og henstillinger og den bedste praksis, der er omhandlet i litra e og f.

For en nærmere gennemgang af kapitel VII om samarbejde og sammenhæng, herunder forordningens artikel 70, henvises til afsnit 8.4.

5.11.3.7. Databeskyttelsesforordningens artikel 40

Det fremgår endvidere af forordningens artikel 40, at sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, kan udarbejde adfærdskodekser eller ændre eller udvide sådanne kodekser med henblik på at specificere anvendelsen af denne forordning, såsom med hensyn til anmeldelsen af brud på persondatasikkerheden til tilsynsmyndighederne og underretningen af de registrerede om sådanne brud på persondatasikkerheden.

5.11.4. Overvejelser

Med databeskyttelsesforordningens artikel 33 indføres – som noget nyt – en generel forpligtelse for alle dataansvarlige til som udgangspunkt at anmelde brud på persondatasikkerhed til tilsynsmyndigheden.

For dataansvarlige omfattet af den særlige telelovgivning vil denne anmeldelsespligt imidlertid ikke være helt ny. Som det fremgår ovenfor, og af de indledende bemærkninger til Kommissionens oprindelige forordningsforslag fra 2012,[597] er forordningens artikel 33 således baseret på kravet om anmeldelse af brud på persondatasikkerheden i artikel 4, stk. 3, i direktivet om e-databeskyttelse. Der er derfor en formodning for, at bestemmelserne har samme indholdsmæssige betydning.

Der er dog to væsentlige forskelle mellem de to regelsæt.[598] Ifølge direktivet om e-databeskyttelse gælder forpligtelsen til at anmelde brud på persondatasikkerheden således samtlige brud; anderledes med databeskyttelsesforordningens artikel 33, hvoraf det som nævnt ovenfor fremgår, at hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, er den dataansvarlige ikke forpligtet til at foretage anmeldelse til tilsynsmyndigheden. Endvidere er fristen for, hvornår der skal være foretaget anmeldelse i direktivet om e-databeskyttelse 24 timer, hvor den i databeskyttelsesforordningens artikel 33 er 72 timer.

[597] Kommisionens forslag af 25. januar (KOM (2012) 11 endelig).

[598] Det bemærkes, at der på nuværende tidspunkt er forhandlinger om en ny e-databeskyttelsesforordning, hvor der i Kommissionens forslag lægges op til, at den særlige underretningspligt – herunder kravet om underretning af den kompetente nationale myndighed om bruddet på persondatabeskyttelsen senest 24 timer efter, at bruddet er påvist – i forbindelse med brud på datasikkerheden ophæves.

Databeskyttelsesforordningens artikel 33 indeholder ikke formkrav til anmeldelse af brud på datasikkerhed til tilsynsmyndigheden. Præambelbetragtning nr. 88 indikerer som nævnt ovenfor, at der kan fastsættes nærmere regler for, hvilket format og hvilke procedurer, der skal anvendes ved anmeldelse af brud på persondatasikkerheden. Det er dog ikke tydeligt hvem, der kan fastsætte nærmere regler om format på anmeldelserne og eventuelle procedurer, som skal følges. Formkrav kan have betydning for både de dataansvarlige, der skal foretage en anmeldelse og for tilsynsmyndigheden, der skal behandle anmeldelserne.

Tilsynsmyndighedens registrering og behandling af anmeldelser om brud på persondatasikkerheden vil formentlig kunne effektiviseres, hvis tilsynsmyndigheden vil kunne fastsætte de nærmere regler for, hvilket format og hvilke procedurer der skal anvendes ved anmeldelser. En sådan standardisering vil således åbne mulighed for, at tilsynsmyndigheden f.eks. – på linje med, hvad der allerede i dag findes på Erhvervsstyrelsens område i forhold til de brud på persondatasikkerheden, som skal anmeldes hertil – vil kunne udbyde en digital løsning via internettet til anmeldelse af brud på persondatasikkerheden. Sådanne nærmere regler vil også kunne være en hjælp til de dataansvarlige, hvis de laves på en sådan måde, at de skaber mere klarhed omkring, hvad og hvordan der skal anmeldes brud på persondatasikkerheden.

Det bør dog i den forbindelse overvejes nærmere, hvorvidt det i alle tilfælde vil være hensigtsmæssigt at forsøge at gøre brug af en eventuel udbudt digital løsning obligatorisk. Hvis en dataansvarlig f.eks. foretager en anmeldelse af et brud på persondatasikkerhed til tilsynsmyndigheden i en e-mail, som indeholder alle de krævede oplysninger i henhold til artikel 33, herunder stk. 3, litra a-d, så er det et åbent spørgsmål, om det vil være muligt for tilsynsmyndigheden med rette at hævde, at der ikke er foretaget lovlig anmeldelse, med henvisning til at anmeldelse skal foretages via en bestemt udbudt digital løsning på internettet. Dette skal ikke mindst ses i lyset af tidsrammerne omkring anmeldelsen og sanktionsbestemmelserne ved overtrædelse af forordningens artikel 33. En anmeldelse af et brud på persondatasikkerheden i en e-mail vil dog skulle overholde de gældende sikkerhedskrav efter forordningen.

Databeskyttelsesforordningens artikel 33, herunder ikke mindst kravet om, at anmeldelsen til tilsynsmyndigheden skal foretages inden for 72 timer, må forventes at indebære, at visse dataansvarlige er nødt til at etablere særlige procedurer til sikring af overholdelse af tidsfristen. Det kan være nødvendigt at sikre, at relevante medarbejdere ved, hvordan der skal reageres ved indmeldelse af et brud på persondatasikkerheden, og rette personer skal kunne vurdere, om der vitterligt er tale om "brud på persondatasikkerheden". Hvad der skal til for at sikre dette er individuelt for den enkelte organisation. Det vil formentlig altid være relevant for den dataansvarlige bl.a. at overveje, hvordan både interne og eksterne henvendel-

ser angående opdagede brud på persondatasikkerheden kan modtages og håndteres, samt rollefordeling.

5.12. Underretning om sikkerhedsbrud til den registrerede, artikel 34

5.12.1 Præsentation

I artikel 34 i databeskyttelsesforordningen fastslås, at når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal den dataansvarlige som udgangspunkt uden unødig forsinkelse underrette den registrerede om bruddet. Gør den dataansvarlige ikke dette, har tilsynsmyndigheden mulighed for at intervenere og kræve, at den dataansvarlige underretter den registrerede om bruddet på persondatasikkerheden.

Der vil i det følgende foretages en gennemgang af gældende ret. Herefter vil der blive redegjort nærmere for indholdet af databeskyttelsesforordningens artikel 34, og det vil i tilknytning hertil blive vurderet, hvilke overvejelser forordningens regel om underretning af den registrerede i tilfælde af brud på persondatasikkerheden vurderes at give anledning til.

5.12.2. Gældende ret

5.12.2.1. Databeskyttelsesdirektivet og persondataloven

Der er hverken i databeskyttelsesdirektivet eller i persondataloven en specifik bestemmelse om underretning af den registrerede i tilfælde af brud på persondatasikkerheden.

Af persondatalovens § 5, stk. 1, fremgår det imidlertid, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik. Denne bestemmelse er baseret på artikel 6, stk. 1, litra a, i databeskyttelsesdirektivet, hvoraf det fremgår, at medlemsstaterne fastsætter bestemmelser om, at personoplysninger skal behandles rimeligt og lovligt.

Det fremgår af forarbejderne til persondataloven, at en rimelig behandling af oplysninger forudsætter bl.a., at registrerede personer kan få kendskab til en behandlings eksistens og, når der indsamles oplysninger hos dem, kan få nøjagtige og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen, jf. §§ 28 og 29. I øvrigt overlades til tilsynsmyndigheden at udfylde den retlige standard "god databehandlingsskik".[599] I Danmark er det primært Datatilsynet, som fastlægger, hvad der skal forstås ved god databehandlingsskik.

[599] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00.

Efter Datatilsynets praksis indebærer kravet om "god databehandlingsskik" i persondatalovens § 5, stk. 1, bl.a., at den dataansvarlige i forbindelse med brud på persondatasikkerheden skal rydde op efter bruddet og søge at begrænse skadevirkningerne heraf.

Ved uberettiget offentliggørelse på internettet skal oplysningerne således fjernes fra hjemmesiden hurtigst muligt, og den ansvarlige må prøve også at få dem fjernet fra Google og andre søgemaskiner. Det kan også være nødvendigt med andre tiltag såsom at sørge for at få fejlagtigt udleverede oplysninger retur fra modtageren eller destrueret hos denne. Afhængigt af de konkrete omstændigheder kan det endvidere være påkrævet, at den dataansvarlige myndighed eller virksomhed tager skridt til, at det langsigtet sikres, at situationen ikke gentager sig, f.eks. ved at interne retningslinjer og forretningsgange kigges efter, ved bedre instruktion af medarbejdere, og/eller ved systemteknisk understøttelse af relevante forretningsgange i organisationen.

Efter Datatilsynets praksis vil det i tilfælde, hvor personoplysninger er kommet til uvedkommendes kendskab eller har været i risiko herfor som følge af et brud på persondatasikkerheden – afhængigt af de konkrete omstændigheder – endvidere følge af persondatalovens grundregel om god databehandlingsskik, at den ansvarlige myndighed eller virksomhed skal underrette de berørte personer.

Ved vurderingen af spørgsmålet om underretning må den dataansvarlige bl.a. tage oplysningernes karakter og de mulige konsekvenser for de berørte personer i betragtning. For så vidt angår spørgsmålet om, hvordan underretningen mest hensigtsmæssigt foretages, må dette ifølge Datatilsynets praksis vurderes i forhold til det skete brud på persondatasikkerheden.[600]

I praksis har Datatilsynet i visse tilfælde spurgt til, om der er foretaget underretning af de berørte personer (de registrerede), eller tilsynet har angivet, at der bør foretages underretning. Dette er sket under hensyntagen til, om underretning af de registrerede viser sig umulig eller er uforholdsmæssigt vanskelig. Tilsynet har på sin hjemmeside også anført, at afhængigt af de konkrete omstændigheder kan det være påkrævet, at den dataansvarlige myndighed eller virksomhed tager skridt til at sørge for en hurtig underretning af berørte personer.

Fra Datatilsynets praksis kan nævnes sagen om uvedkommendes adgang til personoplysninger i Rigspolitiets systemer. Rigspolitiet argumenterede for, at de registrerede personer

[600] På Datatilsynets hjemmeside er en del praksis omkring dette, herunder såvel tilfælde, hvor underretning skulle ske individuelt, som tilfælde, hvor underretning kunne ske via medierne og myndighedens hjemmeside eller helt undlades.

var blevet underrettet, idet sagen havde været omtalt i medierne. Datatilsynet vurderede, at kompromittering af oplysninger fra CPR-registeret kunne have fremgået af visse medier i forbindelse med straffesagen mod hackeren, men tilsynet fandt, at sådanne oplysninger ikke kan anses som fyldestgørende underretning til de berørte om, hvor omfattende data om alle personer og virksomheder i Danmark uvedkommende har haft adgang til. Det var således Datatilsynets opfattelse, at Rigspolitiet – allerede da der fremkom oplysninger om, at Index-registeret var blevet kompromitteret – burde have underrettet de berørte herom, f.eks. ved at informere offentligheden via omtale i medierne eller på politiets hjemmeside. Datatilsynet fandt det beklageligt, at dette ikke var sket. Endvidere mente tilsynet, at Rigspolitiet måtte overveje, om der var anledning til at orientere berørte personer, der på tidspunktet for angrebet var registeret i Schengen-informationssystemet og de øvrige informations-systemer. Det blev fremhævet, at det måtte tages i betragtning, at en del af de registrerede ikke var bosiddende i Danmark, og derfor ikke umiddelbart kan anses for at være blevet informeret via presseomtale i Danmark.[601]

Endvidere kan fra Datatilsynets praksis nævnes en sag, hvor referater fra samtaler mellem en række ansatte og Odder Kommunes arbejdspsykolog over en længere periode havde været lagret på en medarbejders private server, efter at medarbejderen havde overført en række dokumenter fra kommunens netværk til en USB-nøgle og herefter gemt dokumenterne på den private server. Herefter blev oplysningerne tilgængelige for uvedkommende, fordi en anonym person hackede sig ind på serveren. Den anonyme person oplyste selv direkte til medarbejderen, at der lå følsomme personoplysninger på serveren og anbefalede medarbejderen at få det slettet, hvilket medarbejderen straks gjorde. Datatilsynet noterede sig det oplyste om Odder Kommunes overvejelser vedrørende information til de berørte personer og kunne efter omstændighederne tiltræde konklusionen om ikke at fremsende individuel information til de berørte personer. Tilsynet lagde herved vægt på det oplyste om dokumenternes alder, samt at det alene var kommunens arbejdspsykolog, der har kunnet identificere de berørte personer, idet dokumenterne var delvist anonymiserede.[602]

Fra Datatilsynets praksis kan også nævnes en sag, hvor Aalborg Universitet ved en fejl offentliggjorde oplysninger om studerende (bl.a. navne og personnumre) på en hjemmeside. Universitetet argumenterede for ikke at underrette de berørte studerende ved bl.a. at anføre, at den enkelte studerende måtte antages at have været vidende om, at informationerne havde været offentlige, da hjemmesiden havde været brugt som kontaktforum blandt de studerende og deres lærer. Datatilsynet var af den opfattelse, at hvis de berørte personer

[601] Sag vedrørende uvedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er dataansvarlig for, Datatilsynets j.nr. 2013-079-76.
[602] Sag vedrørende uvedkommendes adgang til følsomme oplysninger på en medarbejders private IT-udstyr, Datatilsynets j.nr. 2015-632-0154.

ikke allerede vidste, at deres oplysninger havde været offentliggjort ved en fejl, burde Aalborg Universitet underrette dem om bruddet på persondatasikkerheden, herunder hvilke oplysninger, der har været offentligt tilgængelige på internettet. Tilsynet anmodede på den baggrund Aalborg Universitet om på ny at vurdere, om der - under en eller anden form – skulle ske underretning af de personer, som var berørt af offentliggørelsen.[603]

Herudover kan fra Datatilsynets praksis nævnes en sag, hvor Kommunernes Landsforening havde et brud på persondatasikkerheden i en Cloud-løsning vedrørende et køreprøvesystem. Sikkerhedsbruddet var sket i forbindelse med omlægning af driften af systemet til en Cloud-løsning. Der skete en fejl i opsætningen, som betød, at kørelærere, der loggede på systemet i enkelte perioder, overtog andre samtidige brugeres rettigheder, herunder adgang til oplysninger om de andre kørelærere og disses elever, og i hvert fald tre kørelærere havde som følge heraf haft adgang til andre kørelæreres data. Kommunernes Landsforening oplyste, at de berørte ville blive informeret om hændelsen, men først efter der var overblik over konsekvenserne, og årsagerne til det midlertidige nedbrud var klarlagt. Datatilsynet noterede sig dette.[604]

I en anden sag fra Datatilsynets praksis orienterede Coop Danmark A/S selv tilsynet om, at Irma-torvet A/S havde offentliggjort oplysninger om ca. 35.000 kunders kontaktoplysninger, password og købshistorik på hjemmesiden www.irmatorvet.dk. Som forberedelse til en forventet øget aktivitet på hjemmesiden havde Irmatorvet A/S gennemført tekniske omlægninger og etableret en ekstra stor server til at teste ændringerne på. For at gøre testen så virkelighedstro som muligt, blev der benyttet rigtige kundedata til testen. Serveren var desværre ikke tilstrækkeligt sikkerhedsmæssigt beskyttet, hvilket betød, at kunders kontaktoplysninger og adgangskode til web-butikken i en periode var tilgængelige. Ved logon med adgangskoden kunne oplysninger om kundens købshistorik tilgås. Irmatorvet A/S havde søgt efter kunders kontaktoplysninger mv. på de to store søgemaskiner, Google og Bing, men havde intet fundet. Det var på den baggrund Irmatorvet A/S' vurdering, at de bemeldte sider ikke var blevet indekseret af søgemaskinerne. Vedrørende underretning af de berørte personer oplyste Irmatorvet A/S, at selskabet ville underrette de berørte kunder, såvel privatpersoner som virksomheder/institutioner. Underretning ville ske pr. e-mail. De kunder, der ikke kunne modtage underretningen via e-post, ville få sendt underretningen via almindeligt brev. Datatilsynet fandt det beklageligt, at Irmatorvet A/S ikke havde fulgt tilsynets anbefaling om at tydeliggøre i e-postens emnefelt, at der var tale om en vigtig meddelelse – og ikke en reklame eller et nyhedsbrev. I emnefeltet på den e-post, som blev sendt til Irmatorvet A/S' kunder, fremgik således alene følgende: "Til Irmatorvets kunder".

[603] Sag vedrørende sikkerhedsbrist på Aalborg Universitets hjemmeside, Datatilsynets j.nr. 2007-632-0016.
[604] Sag vedrørende KL's overførsel af et køreprøvesystem til en cloud-løsning, Datatilsynets j.nr. 2011-631-0136.

Datatilsynet noterede sig endvidere det oplyste om, at Irmatorvet A/S ville underrette de berørte personer pr. e-mail, og at Irmatorvet A/S til de kunder, der ikke kunne modtage underretningen via e-post, vil sende underretningen via almindeligt brev.[605]

Fra Datatilsynets praksis kan endelig nævnes en sag, hvor Totalkredit A/S (Totalkredit) havde fremsendt årsopgørelser, der var modtageren uvedkommende. Af årsopgørelserne fremgik oplysninger om navn, adresse, personnummer samt oplysninger om låneforhold. Totalkredit havde pr. brev kontaktet 74 af de 75 personer, om hvem der er udsendt oplysninger til uvedkommende. Den sidste berørte modtager havde Totalkredit været i telefonisk dialog med. Af brevskabelonen, som Totalkredit havde fremsendt til Datatilsynet, fremgik, at der var orienteret om, at den udsendte årsopgørelse var forkert. Meddelelsen indeholdt imidlertid ikke oplysning om, at der havde været et brud på persondatasikkerheden, som havde medført, at kundens oplysninger var gjort tilgængelige for uvedkommende. Datatilsynet fandt, at omstændighederne i denne sag førte til, at Totalkredit skulle informere de berørte personer om bruddet, herunder at oplysninger om deres kundeforhold var sendt til uvedkommende. Datatilsynet lagde herved vægt på, at de oplysninger, som var sendt til uvedkommende omfattede navn, adresse, personnummer samt oplysninger om låneforhold. Der var således tale om ganske omfattende oplysninger, og det kunne efter tilsynets opfattelse ikke udelukkes, at det skete ville kunne få konkrete konsekvenser for de berørte. Datatilsynet anmodede på denne baggrund Totalkredit om at informere de berørte i overensstemmelse med det ovenfor angivne.[606]

5.12.2.2. E-databeskyttelsesdirektivet (direktiv 2002/58/EF) og telelovgivningen[607]

Siden 2011 har telesektoren og virksomheder, som er omfattet af den særlige telelovgivning, været underlagt en pligt til at underrette Erhvervsstyrelsen om brud på persondatasikkerheden, jf. § 8 i lov om elektroniske kommunikationsnet og -tjenester[608] og den i henhold bl.a. hertil udstedte bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

Der er tale om regler, der gennemfører dele af bl.a. Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om databeskyttelse inden for elektronisk kommunikation, som

[605] Sag vedrørende offentliggørelse af kundeoplysninger på www.irmatorvet.dk, Datatilsynets j.nr. 2011-631-0133.
[606] Sag vedrørende sikkerhedsbrist ved udsendelse af årsopgørelser fra Totalkredit A/S, Datatilsynets j.nr. 2008-631-0041.
[607] Generelt kan henvises til bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.
[608] Lovbekendtgørelse nr. 128 af 7. februar 2014, som ændret ved lov nr. 1567 af 15. december 2015.

ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (e-databeskyttelses-direktivet) i dansk ret.[609]

Bekendtgørelsen finder ifølge § 1 anvendelse på styring af risici for persondatasikkerhed og underretning om brud på persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

Ved begrebet "brud på persondatasikkerheden" skal ifølge bekendtgørelsens § 2 forstås sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles i forbindelse med udbuddet af en offentlig elektronisk kommunikationstjeneste.

Af bekendtgørelsens § 5, stk. 1, fremgår, at underretning om brud på persondatasikkerheden skal ske til Erhvervsstyrelsen og i overensstemmelse med artikel 2 i Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden.

Af denne forordnings artikel 3, stk. 1, fremgår, at hvis bruddet på persondatasikkerheden kan forventes at krænke personoplysninger eller privatlivets fred for en abonnent eller en fysisk person, skal udbyderen foruden den underretning, der er nævnt i artikel 2, også underrette abonnenten eller den fysiske person om bruddet.

I forordningens artikel 3, stk. 2, fastslås, at ved vurderingen af, hvorvidt et brud på persondatasikkerheden kan forventes at krænke personoplysninger eller privatlivets fred for en abonnent eller en fysisk person, skal der tages hensyn til *bl.a.* følgende forhold: karakteren og indholdet af de pågældende personoplysninger, navnlig hvor oplysningerne vedrører finansielle oplysninger, særlige kategorier af oplysninger, jf. artikel 8, stk. 1, i databeskyttelsesdirektivet, samt lokaliseringsdata, internet-logfiler, browserhistorik, e-maildata og udspecificerede opkaldslister (litra a), de sandsynlige følger af bruddet på persondatasikkerheden for den berørte abonnent eller fysiske person, navnlig hvis bruddet kan medføre identitetstyveri eller svig, fysisk skade, psykologisk forstyrrelse, tort eller skade af omdømme (litra b) og omstændighederne ved bruddet på persondatasikkerheden, navnlig når oplysningerne er blevet stjålet, eller når udbyderen er bekendt med, at de nødvendige data er i en uautoriseret tredjemands besiddelse (litra c). Der kan i den forbindelse endvidere henvises til forordningens præambelbetragtning nr. 12.

[609] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om databeskyttelse inden for elektronisk kommunikation (EF-Tidende 2002, nr. L 201, s. 37), og Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (EF-Tidende 2009, nr. L 337, s. 11) (e-databeskyttelsesdirektivet).

Forordningen fastsætter ikke – som ved underretning til den kompetente nationale myndighed (i Danmark: Erhvervsstyrelsen) – et eksakt krav til, hvornår underretning til abonnenter eller fysiske personer skal ske rent tidsmæssigt. Underretningen skal ifølge forordningens artikel 3, stk. 3, ske *uden unødig forsinkelse*, efter at bruddet er påvist, og må ikke afhænge af underretningen om bruddet på persondatasikkerheden til tilsynsmyndigheden.

I udbyderens underretning til abonnenten eller den fysiske person vedlægges ifølge forordningens artikel 3, stk. 4, de oplysninger, der er fastsat i bilag II[610]. Underretningen af abonnenten eller den fysiske person skal være udtrykt i et klart og letforståeligt sprog. Udbyderen må ikke bruge underretningen som en lejlighed til at fremme eller reklamere for nye eller supplerende tjenester.

Det fremgår af forordningens artikel 3, stk. 5, at i undtagelsestilfælde, hvor underretningen af abonnenten eller den fysiske person kan bringe en behørig efterforskning af bruddet på persondatasikkerheden i fare, skal udbyderen efter at have opnået samtykke fra den kompetente nationale myndighed (Erhvervsstyrelsen) gives tilladelse til at udskyde underretningen af abonnenten eller den fysiske person, indtil den kompetente nationale myndighed skønner det muligt at underrette om bruddet på persondatasikkerheden i overensstemmelse med denne artikel.

Det fremgår i den forbindelse bl.a. af forordningens præambelbetragtning nr. 13, at undtagelsestilfælde i denne sammenhæng kan omfatte strafferetlig efterforskning samt andre brud på persondatasikkerheden, hvor der ikke er tale om en grov forbrydelse, men for hvilke det kan være hensigtsmæssigt at udskyde underretningen. Det er under alle omstændigheder op til den kompetente nationale myndighed (Erhvervsstyrelsen) – ud fra det enkelte tilfælde og på baggrund af omstændighederne – at tage stilling til, om myndigheden accepterer, at underretningen udskydes eller i det hele taget skal foretages.

I udbyderens underretning til abonnenten eller den fysiske person vedlægges ifølge forordningens artikel 3, stk. 4, de oplysninger, der er fastsat i bilag II[611]. Underretningen af abonnenten eller den fysiske person skal være udtrykt i et klart og letforståeligt sprog. Udbyde-

[611] Udbyderens navn (1). Identitet og kontaktoplysninger for den databeskyttelsesansvarlige eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes (2). Resumé af hændelsen, der forårsagede bruddet på persondatasikkerheden (3) Datoen, hvor hændelsen skønnes at have fundet sted (4). Karakter og indhold af de berørte personoplysninger, jf. artikel 3, stk. 2 (5). Sandsynlige konsekvenser af bruddet på persondatabeskyttelsen for den berørte abonnent eller fysiske person, jf. artikel 3, stk. 2 (6). Omstændigheder ved bruddet på persondatasikkerheden, jf. artikel 3, stk. 2 (7). Foranstaltninger, som udbyderen har sat i værk for at afhjælpe bruddet på persondatabeskyttelsen (8) Foranstaltninger, som udbyderen anbefaler at sætte i værk for at afbøde eventuelle krænkelser (9).

ren må ikke bruge underretningen som en lejlighed til at fremme eller reklamere for nye eller supplerende tjenester.

Udbyderen skal ifølge forordningens artikel 3, stk. 6, i øvrigt underrette abonnenten eller den fysiske person om bruddet på persondatasikkerheden med kommunikationsmidler, som sikrer en hurtig modtagelse af oplysningerne, og som er sikret i overensstemmelse med aktuelle teknikker. Oplysningerne om bruddet skal stå alene og må ikke gives sammen med oplysninger om andre emner, jf. også forordningens præambelbetragtning nr. 15, hvoraf det bl.a. fremgår, at det eksempelvis ikke betragtes som et velegnet middel til at underrette om et brud på persondatasikkerheden, hvis en normal faktura benyttes til at underrette om et brud på persondatasikkerheden.

Af forordningens artikel 3, stk. 7, fremgår, at hvis udbyderen, som har et direkte kontraktforhold til slutbrugeren, på trods af rimelige bestræbelser er ude af stand til inden for den tidsfrist, der er angivet i stk. 3, at identificere alle fysiske personer, som må forventes at blive krænket af bruddet på persondatasikkerheden, kan udbyderen underrette disse personer gennem annoncer i større nationale eller regionale medier i de relevante medlemsstater inden for tidsfristen. Disse annoncer skal indeholde de oplysninger, der er angivet i bilag II, om nødvendigt i sammenfattet form. I dette tilfælde skal udbyderen videreføre rimelige bestræbelser på at identificere disse fysiske personer og underrette dem om de i bilag II angivne oplysninger hurtigst muligt.

Der henvises i den forbindelse endvidere til præambelbetragtning nr. 14 i forordningen, hvoraf det bl.a. fremgår, at udbydere må forventes at have rådighed over deres abonnenters kontaktoplysninger i lyset af deres direkte kontraktforhold, men sådanne oplysninger findes muligvis ikke for andre fysiske personer, der berøres af bruddet på persondatasikkerheden. I det tilfælde bør der gives tilladelse til, at udbyderen i første omgang underretter disse fysiske personer via annoncer i større nationale eller regionale medier, f.eks. aviser, og at disse hurtigst muligt efterfølges af en individuel underretning som fastsat ved denne forordning. Udbyderen forpligtes derfor ikke til at underrette gennem medierne, men får snarere beføjelse til at handle på denne måde, hvis udbyderen ønsker det, når vedkommende stadig er i færd med at identificere alle fysiske personer.

Forordningens artikel 4, stk. 1, slår endvidere fast, at uanset artikel 3, stk. 1, er det ikke nødvendigt at underrette den pågældende abonnent eller fysiske person om et brud på persondatasikkerheden, hvis den kompetente nationale myndighed finder det godtgjort fra udbyderens side, at denne har gennemført passende teknologiske beskyttelsesforanstaltninger, og at disse foranstaltninger er blevet anvendt på de data, som sikkerhedsbruddet ved-

rørte. Sådanne teknologiske beskyttelsesforanstaltninger skal gøre dataene uforståelige for alle, der ikke har lovlig adgang hertil.

Data anses ifølge forordningens artikel 4, stk. 2, for uforståelige, hvis: a) de er blevet krypteret på sikker vis med en standardiseret algoritme, dekrypteringsnøglen ikke er kompromitteret af et brud på sikkerheden, og dekrypteringsnøglen er genereret på en sådan måde, at den ikke kan afsløres med de tilgængelige tekniske midler af en person, der ikke har lovlig adgang til nøglen, eller b) de er blevet erstattet af deres hashværdi, der beregnes med en standardiseret kryptografisk hashfunktion med en nøgle, den nøgle, der er anvendt til at "hashe" dataene, ikke er kompromitteret af et brud på sikkerheden, og den nøgle, der er anvendt til at "hashe" dataene, er genereret på en sådan måde, at den ikke kan afsløres med de tilgængelige tekniske midler af en person, der ikke har lovlig adgang til nøglen

Det fremgår endelig af forordningens artikel 5, at hvis en udbyder indgår en kontrakt med en anden udbyder om at levere en del af de elektroniske kommunikationstjenester uden at have et direkte kontraktforhold til abonnenter, skal denne anden udbyder øjeblikkeligt oplyse den kontraherende udbyder om brud på persondatasikkerheden.

Bestemmelsen er uddybet i forordningens præambelbetragtning nr. 18. Det følger bl.a. heraf, at hvis en udbyder – f.eks. en såkaldt "service provider" - benytter en anden udbyder til at udføre en del af tjenesteydelsen, f.eks. i forbindelse med fakturering og ledelsesfunktioner, bør denne anden udbyder, som ikke har et direkte kontraktforhold til slutbrugeren, ikke være forpligtet til at foretage underretninger i tilfælde af brud på persondatasikkerheden. Den anden udbyder bør i stedet advare og oplyse den udbyder, der har det direkte aftaleforhold med abonnenterne, således at denne kan foretage underretningen.

Hvis Erhvervsstyrelsen konstaterer, at en udbyder ikke har underrettet eventuelt berørte abonnenter eller fysiske personer, kan Erhvervsstyrelsen – efter at have vurderet de sandsynlige negative virkninger af bruddet – kræve, at udbyderen underretter abonnenten eller den fysiske person om sikkerhedsbruddet, jf. bekendtgørelsens § 5, stk. 2.

For en nærmere gennemgang af forpligtelsen til at foretage underretning til Erhvervsstyrelsen i tilfælde af brud på persondatasikkerheden og den generelle underretningspligt, der vil komme til at gælde efter den 25. maj 2018, når databeskyttelsesforordningen finder anvendelse, jf. forordningens artikel 33, henvises til afsnit 5.11. Der er i dette afsnit endvidere redegjort nærmere for det forslag til til Europa-Parlamentets og Rådets forordning om respekten for privatlivet og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om privatlivets fred

og elektronisk kommunikation) (KOM/2017/010 endelig), som Kommissionen har fremlagt den 10. januar 2017.

5.12.2.3. Udtalelse fra Artikel 29-gruppen om underretning om brud på persondatasikkerheden

Artikel 29-gruppen har i 2014 udarbejdet en udtalelse 03/2014 om underretning om brud på persondatasikkerheden.[612]

Der er ifølge udtalelsens resumé tale om en vejledning til de dataansvarlige for at hjælpe dem med at afgøre, om de skal underrette registrerede i tilfælde af "brud på persondatasikkerheden". Udtalelsen omhandler de eksisterende forpligtelser for udbydere af elektroniske kommunikationstjenester i medfør af direktiv 2002/58/EF. Den giver samtidig eksempler fra forskellige sektorer, som er relevante for udkastet til en forordning om databeskyttelse, og beskriver god praksis for alle dataansvarlige. Hvor underretning af den kompetente myndighed kræves i alle tilfælde af brud på datasikkerheden i henhold til direktiv 2002/58/EF, er fokus i denne udtalelse fra Artikel 29-gruppen ifølge resuméet at analysere brud på persondatasikkerheden, der kræver underretning af de registrerede. Endvidere beskrives det, hvordan de dataansvarlige i første omgang kunne have sikret deres systemer, så de kunne have undgået bruddet på persondatasikkerheden, eller hvilke foranstaltninger de i det mindste kunne have gennemført for at blive fritaget for pligten til at underrette de registrerede. Udtalelsen besvarer også nogle af de mest almindelige spørgsmål vedrørende brud på persondatasikkerheden og anvendelsen af direktiv 2002/58/EF.

Der opstilles i udtalelsen endvidere en ikke-udtømmende liste over tilfælde, hvor registrerede bør underrettes. Hvert brud på persondatasikkerheden undersøges på grundlag af tre klassiske sikkerhedsbrud. Udtrykket "brud på tilgængelighed" svarer således til hændelig eller ulovlig tilintetgørelse eller tab af personoplysninger, "brud på integritet" svarer til ændring af personoplysninger, og "brud på fortrolighed" svarer til ubeføjet videregivelse af eller adgang til personoplysninger. I udtalelsen gives der derefter generel vejledning om tilfælde, der ikke kræver underretning. Endelig omhandler udtalelsen de forhold, som dataansvarlige især skal tage i betragtning, når de overvejer, om registrerede skal underrettes.

5.12.3. Databeskyttelsesforordningen

5.12.3.1. Databeskyttelsesforordningens artikel 34, stk. 1

Det følger af forordningens artikel 34, stk. 1, at når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder – så som diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme,

[612] Artikel 29-gruppens udtalelse nr. 3/2014 om underretning om brud på persondatasikkerheden (WP 213).

tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede – skal den dataansvarlige underrette den registrerede om bruddet på persondatasikkerheden. Dette skal ske uden unødig forsinkelse.

Det bemærkes, at alle de mulige konsekvenser og negative virkninger for de registrerede bør tages i betragtning. I den ovenfor nævnte udtalelse fra Artikel 29-gruppen er således på side 13 omtalt et eksempel, hvor et musikselskabs websted er blevet hacket, og dets brugerdatabase er blevet stjålet og offentliggjort på internettet. De lækkede personoplysninger består af navne/efternavne, musikpræferencer samt brugernavne og adgangskoder for de brugere, der har registreret sig på selskabets websted. 9.000 brugere er berørt. I forbindelse med dette brud kan den direkte negative virkning for de enkelte ifølge Artikel 29-gruppen forekomme ret begrænset i de fleste tilfælde (dvs. lækage af information om musikpræferencer) og kan give anledning til at overveje, om de registrerede skal underrettes. Da adgangskoderne blev kompromitteret, skal de dog fornys af den dataansvarlige. I denne proces vil det være nødvendigt at informere brugerne om årsagen til, at adgangskoderne skal fornys. Eftersom mange brugere anvender den samme adgangskode på forskellige konti, vil bruddet som en sekundær negativ virkning sandsynligvis også medføre et brud på fortroligheden i forbindelse med en anden konto. De registrerede vil kunne minimere disse sekundære virkninger ved at skifte adgangskode på alle deres andre konti. Underretningen skal derfor også indeholde oplysninger om de sandsynlige negative virkninger i forbindelse med andre konti og bør derfor omfatte en anbefaling om at bruge forskellige adgangskoder på forskellige websteder og om at forny adgangskoderne til konti, hvor den kompromitterede adgangskode blev anvendt.

Den dataansvarlige skal endvidere, afhængigt af de sandsynlige negative virkninger, foretage underretning, uanset antallet af berørte registrerede.

Som det fremgår af ordlyden af forordningens artikel 34, stk. 1, indeholder bestemmelsen ikke – som ved kravet om anmeldelse af et brud på persondatasikkerheden til tilsynsmyndigheden i forordningens artikel 33 – et eksakt krav til, hvornår underretning til den registrerede skal ske rent tidsmæssigt. Underretningen skal ske *uden unødig forsinkelse*, efter at bruddet er påvist, og må antages ikke at afhænge af underretningen om bruddet på persondatasikkerheden til tilsynsmyndigheden.

Kravet om underretning uden unødig forsinkelse bør i øvrigt også ses i sammenhæng med formålet med underretningen, som ifølge præambelbetragtning nr. 86 er ”at give den registrerede mulighed for at træffe de fornødne forholdsregler”.

Det fremgår i den forbindelse også af præambelbetragtning nr. 86, at underretninger til registrerede bør gives, så snart det med rimelighed er muligt og i tæt samarbejde med tilsynsmyndigheden, i overensstemmelse med retningslinjer, der er udstukket af denne eller af andre relevante myndigheder, såsom de retshåndhævende myndigheder. Eksempelvis kræver behovet for at begrænse en umiddelbar risiko for skade omgående underretning af registrerede, mens behovet for at gennemføre passende foranstaltninger mod fortsatte eller lignende brud på persondatasikkerheden kan begrunde en længere frist for underretning.

Hvis bruddet på persondatasikkerheden f.eks. består i en offentliggørelse af den registreredes beskyttede fysiske adresse, og adressen netop er beskyttet, fordi den registrerede risikerer fysisk vold fra en anden person, så kan det selvsagt være af afgørende betydning, hvornår den registrerede får underretningen om offentliggørelsen.

I andre tilfælde kan tiden være mindre kritisk, men det kan stadig gøre en forskel på den måde, at en hurtigere underretning kan give den registrerede bedre mulighed for at beskytte sig selv. Det er f.eks. ikke ualmindeligt, at mange mennesker bruger den samme kombination af brugernavn og adgangskode til mange internetkonti, og er disse oplysninger blevet kompromitteret i forbindelse med et brud på persondatasikkerheden hos en dataansvarlig, således at en tredjemand nu kender oplysningerne, vil tredjemanden sandsynligvis kunne få adgang til andre konti tilhørende den pågældende registrerede, herunder i nogle tilfælde e-mail-konti. Konsekvenserne for den registrerede kan i et sådant tilfælde eventuelt begrænses, jo hurtigere vedkommende underrettes om bruddet på persondatasikkerheden med en klar anbefaling om at ændre adgangskoder til alle de konti, der deler den samme kompromitterede adgangskode.

5.12.3.2. Databeskyttelsesforordningens artikel 34, stk. 2

Af forordningens artikel 34, stk. 2, følger, at underretningen af den registrerede i henhold til stk. 1 i et klart og forståeligt sprog skal beskrive karakteren af bruddet på persondatasikkerheden og mindst indeholde de oplysninger og foranstaltninger, der er omhandlet i artikel 33, stk. 3, litra b, c og d.

Kravet om, at underretningen skal ske i et klart og forståeligt sprog, er i tråd med formålet med at orientere den registrerede om bruddet på persondatasikkerheden, jf. det ovenfor anførte, herunder præambelbetragtning nr. 86. Hvis underretningen ikke er forståelig for den registrerede, vil vedkommende have vanskeligt ved at træffe de fornødne forholdsregler.

Henvisningen til artikel 33, stk. 3, litra b, c og d i forordningens artikel 34, stk. 2, indebærer, at underretningen til den registrerede som minimum skal indeholde:

b) angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
c) beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
d) beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Der er tale om en ikke-udtømmende opregning af, hvilke oplysninger der skal gives, jf. ordet "minimum".

5.12.3.3. Databeskyttelsesforordningens artikel 34, stk. 3

Det er efter forordningens artikel 34, stk. 3, ikke nødvendigt at underrette den registrerede som omhandlet i stk. 1, hvis en af følgende betingelser er opfyldt:

a) den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering
b) den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1 sandsynligvis ikke længere er reel
c) det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

Som et eksempel på, hvad der kan give den dataansvarlige anledning til at vurdere, om underretning af den registrerede kan undlades i henhold til artikel 34, stk. 3, *litra a*, kan nævnes en situation, hvor en dataansvarlig har mistet et bærbart medie, hvorpå der er lagret persondata i krypteret form. Der kan være anvendt en tilstrækkelig stærk kryptering, som ikke kan brydes eller omgås inden for en tilstrækkelig lang årrække, og uvedkommende har ikke og får ikke mulighed for at dekryptere data på normal vis – f.eks. ved at komme i besiddelse af rette krypteringsnøgle. Den dataansvarlige kan i så fald siges at have en formodning om, at persondata er beskyttet på en sådan måde, at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

I forhold til artikel 34, stk. 3, *litra b*, kunne et eksempel på, hvad der kan give den dataansvarlige anledning til at vurdere, om underretning af den registrerede kan undlades, være, at et IT-system opdateres, og denne opdatering resulterer i, at der utilsigtet etableres adgang til fortrolige persondata fra internettet, uden login (dvs. uden autorisation af brugeren). Herved bliver der i et tidsrum mulig adgang for uautoriserede personer til persondata fra internettet. Den dataansvarlige opdager selv efterfølgende, at bruddet på persondatasikkerhed er sket og afskærer herefter straks adgangen for uautoriserede brugere, så persondata ikke længere er eksponeret. Endvidere iværksætter den dataansvarlige straks en undersøgelse af de nærmere omstændigheder ved bruddet på persondatasikkerheden. Undersøgelsen dokumenterer med sikkerhed, i hvilket tidsrum data har været tilgængelige for uautoriserede personer. Undersøgelsen dokumenterer også, at der findes troværdige logs, som ikke kan omgås og som har logget, når personoplysninger blev tilgået i tidsrummet, hvor persondata var eksponeret. Det kan endvidere på grundlag af de troværdige logoplysninger dokumenteres, at kun autoriserede brugere faktisk har tilgået persondata, mens de var eksponeret – dvs. i det tidsrum, hvor bruddet på persondatasikkerheden stod på.

Der henvises i øvrigt til den ovenfor omtalte udtalelse fra Artikel 29-gruppen om underretning om brud på persondatasikkerheden.[613] Denne udtalelse beskriver således bl.a., hvordan de dataansvarlige i første omgang kunne have sikret deres systemer, så de kunne have undgået bruddet på persondatasikkerheden, eller hvilke foranstaltninger de i det mindste kunne have gennemført for at blive fritaget for pligten til at underrette de registrerede, ligesom den indeholder generel vejledning om tilfælde, der ikke kræver underretning. Endelig omhandler udtalelsen de forhold, som dataansvarlige især skal tage i betragtning, når de overvejer, om registrerede skal underrettes.

Bevisbyrden for, at en af betingelserne i forordningens artikel 34, stk. 3, litra a-c var opfyldt, påhviler den dataansvarlige. Dette kan blive aktuelt senere, f.eks. i forbindelse med en sag hos tilsynsmyndigheden, hvor den dataansvarlige således skal være i stand til at begrunde, hvorfor anmeldelse af bruddet på persondatasikkerheden til tilsynsmyndigheden blev fravalgt.

Der kan endvidere ifølge forordningens artikel 23, stk. 1, gøres undtagelser fra underretningspligten i artikel 34 ud fra hensyn til bl.a. statens sikkerhed.

Herudover indeholder forordningens artikel 12, stk. 1, en række generelle betingelser for, hvordan den dataansvarlige skal kommunikere omkring bl.a. artikel 34, ligesom forordnin-

[613] Artikel 29-gruppens udtalelse nr. 3/2014 om underretning om brud på persondatasikkerheden (WP 213).

gens artikel 12, stk. 5, bl.a. slår fast, at enhver meddelelse og enhver foranstaltning, der træffes i henhold til artikel 34, er gratis.

5.12.3.4. Databeskyttelsesforordningens artikel 34, stk. 4
Af forordningens artikel 34, stk. 4, fremgår det, at hvis den dataansvarlige ikke allerede har underrettet den registrerede om bruddet på persondatasikkerheden, kan tilsynsmyndigheden efter at have overvejet sandsynligheden for, at bruddet på persondatasikkerheden indebærer en høj risiko, kræve, at den dataansvarlige gør dette, eller beslutte, at en af betingelserne i artikel 34, stk. 3 er opfyldt.

Der henvises i den forbindelse også til forordningens artikel 58, stk. 2, litra e, hvorefter tilsynsmyndigheden har korrigerende beføjelser til blandt andet at give den dataansvarlige påbud om at underrette den registrerede om et brud på persondatasikkerheden.

5.12.3.5. Databeskyttelsesforordningens artikel 70, stk. 1, litra e, litra h og litra l
Af forordningens artikel 70, stk. 1, litra e, fremgår det i øvrigt, at Databeskyttelsesrådet på eget initiativ, efter anmodning fra et af sine medlemmer eller efter anmodning fra Kommissionen skal undersøge ethvert spørgsmål vedrørende anvendelsen af denne forordning og udstede retningslinjer, henstillinger og bedste praksis for at fremme ensartet anvendelse af denne forordning.

I forordningens artikel 70, stk. 1, litra f – m, opregnes herefter en række områder, hvor rådet skal udstede sådanne retningslinjer, henstillinger og bedste praksis i overensstemmelse med litra e. Et af de nævnte områder er: de omstændigheder, hvor brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder som omhandlet i artikel 34, stk. 1, jf. litra h.

De omhandlede retningslinjer mv. er ikke bindende for medlemsstaterne, men vil formentlig få en vis normerende effekt for de nationale tilsynsmyndigheder og må dermed antages at komme til at medvirke til at øge graden af harmonisering af udmøntningen af forordningens regler i medlemsstaterne.

Det fremgår endvidere af forordningens artikel 70, stk. 1, litra l, at Databeskyttelsesrådet skal gennemgå den praktiske anvendelse af de retningslinjer og henstillinger og den bedste praksis, der er omhandlet i bl.a. litra e.

5.12.3.6. Databeskyttelsesforordningens artikel 40
Det fremgår endvidere af forordningens artikel 40, at sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, kan udarbejde ad-

færdskodekser eller ændre eller udvide sådanne kodekser med henblik på at specificere anvendelsen af denne forordning, såsom med hensyn til anmeldelsen af brud på persondatasikkerheden til tilsynsmyndighederne og underretningen af de registrerede om sådanne brud på persondatasikkerheden.

5.12.4. Overvejelser

Med databeskyttelsesforordningens artikel 34 kodificeres forpligtelsen til som udgangspunkt at underrette registrerede i tilfælde af brud på persondatasikkerheden. Der er dermed tale om en tydeliggørelse af den underretningsforpligtelse, som i dag for de dataansvarlige udledes af persondatalovens grundregel om god databehandlingsskik og Datatilsynets praksis.

Bestemmelsen formaliserer samtidig tilsynsmyndighedens forpligtelser på dette område. Fremover skal tilsynsmyndigheden således i et tæt samarbejde med den dataansvarlige påse, at der gives underretninger til registrerede, jf. præambelbetragtning nr. 86, og dette i overensstemmelse med retningslinjer, der er udstukket af enten tilsynsmyndigheden eller af andre relevante myndigheder, såsom de retshåndhævende myndigheder. Tilsynsmyndigheden skal endvidere tage stilling til, hvorvidt den – i tilfælde af, at den dataansvarlige ikke allerede har underrettet den registrerede om bruddet på persondatasikkerheden – efter at have overvejet sandsynligheden for, at bruddet på persondatasikkerheden indebærer en høj risiko, skal kræve, at den dataansvarlige gør dette, eller beslutte, at en af betingelserne i artikel 34, stk. 3 er opfyldt, jf. artikel 34, stk. 4.

Hvor det i dag kun er i forhold til de dataansvarlige, der er omfattet af den særlige telelovgivning, der er lovgivningsmæssigt forpligtet til at anmelde brud på persondatasikkerheden til Erhvervsstyrelsen og efter omstændigheder også underrette abonnenter mv., bliver denne anmeldelsesforpligtelse med databeskyttelsesforordningens artikel 33 nu – som noget nyt – generel. Det betyder, at den kommer til at gælde for alle sektorer, dvs. både for offentlige myndigheder og private virksomheder – og ikke kun som i dag for telesektoren. Der vil i forbindelse med en anmeldelse af et brud på persondatasikkerheden til tilsynsmyndigheden efter databeskyttelsesforordningen i hvert enkelt tilfælde også skulle tages stilling til forordningens artikel 34 om underretning af brud på persondatasikkerheden til den registrerede.

5.13. Konsekvensanalyser vedrørende databeskyttelse, artikel 35

5.13.1. Præsentation

Forordningens artikel 35 indeholder et krav om, at hvis en behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal den dataansvarlige forud for behandlingen foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger. Artiklen indeholder endvidere de nærmere krav til en konsekvensanalyse vedrørende databeskyttelse. Pligten til at foretage en konsekvensanalyse gælder alene i særlige tilfælde, hvor der kan konstateres en høj risiko.

5.13.2. Gældende ret

Hverken databeskyttelsesdirektivet, persondataloven eller sikkerhedsbekendtgørelsen indeholder krav om konsekvensanalyser eller lister over behandlingsaktiviteter, der kræver (eller ikke kræver) konsekvensanalyser.[614]

Datatilsynet har imidlertid i en række udtalelser anbefalet, at der udarbejdes konsekvensanalyser.[615]

Fra Datatilsynets praksis kan nævnes et høringssvar vedrørende ændring af pasloven, som blev afgivet til Justitsministeriet, hvori Datatilsynet opfordrer til, at der gennemføres en såkaldt privatlivsimplikationsanalyse (Privacy Impact Assessment eller PIA), hvor alle elementer i løsningen analyseres, og at der bør sikres procedure og garantier til beskyttelse af oplysningerne og til imødegåelse af risici i forhold til borgernes ret til beskyttelse af personoplysninger og privatliv.[616]

Digitaliseringsstyrelsen har udarbejdet en vejledning til brug for vurdering af offentlige IT-projekters potentielle konsekvenser for privatlivet[617] samt en guide til konsekvensvurdering af privatlivsbeskyttelse[618]. Vejledningerne er udarbejdet til offentlige myndigheder, men kan naturligvis også anvendes af private virksomheder.

---

[614] Der findes forskellige definitioner af begreberne Privacy Impact Assesstment, Data Privacy Impact Assesstment, Data Protection Impact Assessment og Konsekvensanalyse, men de kan eksempelvis findes defineret her: DS/ISO/IEC 27000, 4. udgave, 2014-02-10.
[615] Datatilsynets j.nr. 2010-112-0288, Datatilsynets j.nr. 2012-112-0011, Datatilsynets j.nr. 2013-112-0268.
[616] Høring over ændring af pasloven, Datatilsynets j.nr. 2011-111-0069.
[617] "Vejledning i vurdering af offentlige IT-projekters potentielle konsekvenser for privatlivet" udgivet af Digitaliseringsstyrelsen, maj 2013.
[618] "Guide til konsekvensvurdering af privatlivsbeskyttelse" udgivet af Digitaliseringsstyrelsen, maj 2013. Der findes forskellige definitioner af begreberne Privacy Impact Assesstment, Data Privacy Impact Assesst-

Konsekvensanalyser har således ikke tidligere været reguleret i lovgivningen, men er blevet anbefalet af Datatilsynet i specifikke situationer og gennem vejledninger fra Digitaliseringsstyrelsen. Der er således ikke med selve betegnelsen "konsekvensanalyse" tale om en nyskabelse, da udarbejdelse af konsekvensanalyser har været anbefalet i praksis.

5.13.3. Databeskyttelsesforordningen

Forordningens artikel 35 indeholder krav om, at der i visse tilfælde skal udarbejdes konsekvensanalyser vedrørende databeskyttelse.

Det fastsættes generelt i artikel 35, stk. 1, hvornår en dataansvarlig skal foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger. Artikel 35, stk. 3, specificerer nærmere de tilfælde, hvor en konsekvensanalyse navnlig er påkrævet. Artikel 35, stk. 7, fastsætter, hvad en konsekvensanalyse mindst skal omfatte. Endelig fastsætter artikel 35, stk. 11, hvornår det er nødvendigt at foretage en fornyet konsekvensanalyse.

5.13.3.1. Databeskyttelsesforordningens artikel 35, stk. 1

Det fremgår af artikel 35, stk. 1, at hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger. En enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici.

Det følger af præambelbetragtning nr. 84, at for at fremme overholdelse af denne forordning bør den dataansvarlige, hvor behandlingsaktiviteter sandsynligvis indebærer en høj risiko for fysiske personers rettigheder og frihedsrettigheder, have ansvaret for at foretage en konsekvensanalyse vedrørende databeskyttelse for navnlig at vurdere denne risikos oprindelse, karakter, særegenhed og alvor. Resultatet af analysen bør tages i betragtning, når der skal træffes passende foranstaltninger med henblik på at påvise, at behandlingen af personoplysningerne overholder denne forordning. Hvis det fremgår af en konsekvensanalyse vedrørende databeskyttelse, at behandlingsaktiviteter indebærer en høj risiko, som den dataansvarlige ikke kan begrænse ved passende foranstaltninger med hensyn til tilgængelig teknologi og gennemførelsesomkostninger, bør tilsynsmyndigheden høres forud for behandlingen.

---

ment og Konsekvensanalyse, men de kan eksempelvis findes defineret i DS/ISO/IEC 27000, 4. udgave, 2014-02-10 .

Det følger endvidere af præambelbetragtning nr. 89, at der ved databeskyttelsesdirektivet blev fastsat en generel forpligtelse til at anmelde behandlingen af personoplysninger til tilsynsmyndighederne. Denne forpligtelse medførte en administrativ og finansiel byrde, men den bidrog ikke i alle tilfælde til at forbedre beskyttelsen af personoplysninger. En sådan vilkårlig og generel anmeldelsespligt bør derfor afskaffes og erstattes med effektive procedurer og mekanismer, som i stedet fokuserer på de typer behandlingsaktiviteter, der sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder i medfør af deres karakter, omfang, sammenhæng og formål. Sådanne typer behandlingsaktiviteter kan være aktiviteter, der navnlig indebærer brug af ny teknologi, eller aktiviteter, som er af en ny slags, og hvor den dataansvarlige endnu ikke har foretaget en konsekvensanalyse vedrørende databeskyttelse, eller hvor de er blevet nødvendige på grund af den tid, der er gået siden den oprindelige behandling.

I forlængelse heraf følger det af præambelbetragtning nr. 90, at den dataansvarlige i sådanne tilfælde inden behandlingen bør foretage en konsekvensanalyse vedrørende databeskyttelse med henblik på at vurdere den høje risikos specifikke sandsynlighed og alvor under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt risikokilderne. Konsekvensanalysen bør navnlig omfatte de foranstaltninger, garantier og mekanismer, der er planlagt til begrænsning af denne risiko, til sikring af beskyttelsen af personoplysninger og påvisning af overholdelse af denne forordning.

Endelig følger det af præambelbetragtning nr. 93, at medlemsstaterne i forbindelse med vedtagelsen af national lovgivning i medlemsstaterne, der udgør grundlaget for en offentlig myndigheds eller et offentligt organs udførelse af opgaver, og som regulerer den eller de pågældende specifikke behandlingsaktiviteter, kan vurdere, at en sådan analyse skal foretages inden behandlingsaktiviteterne.

Som det fremgår af artikel 35, stk. 1, kan det *navnlig* være relevant at vurdere behovet for en konsekvensanalyse, hvis der er tale om en type behandling, som indebærer brug af nye teknologier.

”Nye teknologier” kan eksempelvis være brugen af biometriske data, herunder anvendelse af iris-scanning, eller af kunstig intelligens, men også adgangen til eksempelvis at kommunikere med det offentlige via apps på mobile enheder eller brug af elektroniske identiteter.

Med ”ny teknologi” skal der være tale om objektivt set ny teknologi. Det forhold, at der for den dataansvarlige konkret er tale om ny teknologi i form af eksempelvis skift af IT-platform, kan ikke i sig selv være afgørende for, at der skal udarbejdes en konsekvensana-

lyse, hvis ikke der derved vurderes at være en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

Kategorien af personoplysninger skal ses i sammenhæng med den valgte behandlingsaktivitet. Eksempelvis bør der, inden behandlingen påbegyndes udarbejdes en konsekvensanalyse, hvis der er tale om en behandlingsaktivitet, som bruger en ny teknologi, der skal behandle en eller flere forskellige personoplysninger, som er reguleret i artikel 9. Et eksempel på anvendelse af ny teknologi kan være, når kunstig intelligens anvendes til at diagnosticere patienter og efterfølgende anbefale en behandling.

Det er imidlertid ikke et krav, at der skal være tale om brug af nye teknologier. Der bør derfor også, i de tilfælde, hvor der ikke gøres brug af nye teknologier, konkret tages stilling til, om en behandling sandsynligvis vil indebære en høj risiko.

Det følger af artikel 35, stk. 1, at der alene skal foretages en konsekvensanalyse, når der sandsynligvis vil være *høj risiko* for fysiske personers rettigheder og frihedsrettigheder. Dette må antageligvis indebære, at artikel 35 vil have et forholdsvis begrænset anvendelsesområde. Den dataansvarlige vil således i de fleste tilfælde ikke skulle foretage en konsekvensanalyse. Dette skal ses i lyset af, at det formentlig kun vil være i få tilfælde, at der konstateres en høj risiko, jf. også nedenfor om artikel 35, stk. 3.

Om risikovurdering fremgår det af bl.a. præambelbetragtning nr. 75, at risiciene for fysiske personers rettigheder og frihedsrettigheder, af varierende sandsynlighed og alvor, kan opstå som følge af behandling af personoplysninger, hvis de registrerede kan blive berøvet deres rettigheder og frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger; hvis der behandles personoplysninger, der viser race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, og behandling af genetiske data, helbredsoplysninger eller oplysninger om seksuelle forhold eller straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger; hvis personlige forhold evalueres, navnlig analyse eller forudsigelse af forhold vedrørende indsats på arbejdspladsen, økonomisk situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografisk position eller bevægelser, med henblik på at oprette eller anvende personlige profiler; hvis der behandles personoplysninger om sårbare fysiske personer, navnlig børn; eller hvis behandlingen omfatter en stor mængde personoplysninger og berører et stort antal registrerede.

Af præambelbetragtning nr. 76 fremgår det endvidere, at risikoens sandsynlighed og alvor for så vidt angår den registreredes rettigheder og frihedsrettigheder bør bestemmes med henvisning til behandlingens karakter, omfang, sammenhæng og formål. Risikoen bør eva-

lueres på grundlag af en objektiv vurdering, hvorved det fastslås, om databehandlingsaktiviteter indebærer en risiko eller en høj risiko.

Den dataansvarlige skal i forbindelse med udarbejdelsen af en konsekvensanalyse inddrage de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger. Det bør eksempelvis vurderes, hvilke konsekvenser et brud på persondatasikkerheden vil kunne medføre i forhold til den valgte behandlingsaktivitet. Mængden af data skal også vurderes i forhold til den valgte behandlingsaktivitet og indgå i vurderingen af, om en identificeret risiko må karakteriseres som værende høj.

Det fremgår af forordningens artikel 35, stk. 1, 2. pkt., at en enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici.

Det fremgår af præambelbetragtning nr. 92, at der kan være tilfælde, hvor det kan være rimeligt og økonomisk at foretage en konsekvensanalyse vedrørende databeskyttelse, som omfatter mere end ét enkelt projekt, f.eks. hvis offentlige myndigheder eller organer har planer om at indføre en fælles applikation eller behandlingsplatform, eller hvis flere dataansvarlige planlægger at indføre en fælles applikation eller behandlingsplatform på tværs af en industrisektor eller et industrisegment eller for en udbredt horisontal aktivitet.

Artikel 35, stk. 1, 2. pkt., må antageligvis betyde, at det kan være tilstrækkeligt at udarbejde en konsekvensanalyse for flere lignede behandlingsaktiviteter, uanset størrelsen af den samlede mængde af data, som behandlingsaktiviteterne omfatter.

Endvidere må det betyde, at flere dataansvarlige kan foretage en fælles konsekvensanalyse vedrørende databeskyttelse (dog således, at de hver især har ansvaret herfor), forudsat at der er tale om samme type system, den samme behandlingsaktivitet af de samme personoplysninger, samt at det indebærer lignende høje risici.

Det vil eksempelvis være tilstrækkeligt for flere kommuner at udarbejde én konsekvensanalyse vedrørende databeskyttelse i det samme system (som leveres af samme leverandør), hvis systemet behandler de samme typer af personoplysninger og behandlingsaktiviteterne indebærer samme høje risici.

Det er de dataansvarlige, der konkret vurderer, hvorvidt systemerne og behandlingsaktiviteterne er identiske, herunder gennem en vurdering af indkøbstidspunkt af varierende system-versioner, leverandør mv. Såfremt systemerne vurderes ikke at være identiske eller tilnærmelsesvis identiske, skal de dataansvarlige som udgangspunkt foretage en selvstæn-

dig konsekvensanalyse. Det afgørende er således ikke, at der er fuld identitet, men at systemet og data ikke afviger væsentligt fra hinanden.

Et eksempel på, at der ikke foreligger den fornødne identitet mellem flere systemer er den situation hvor en dataansvarlig foretager et tilkøb til et system. Et sådan tilkøb vil umiddelbart ikke være omfattet af en generel konsekvensanalyse for det pågældende system.

5.13.3.2. Databeskyttelsesforordningens artikel 35, stk. 2
Det fremgår af forordningens artikel 35, stk. 2, at den dataansvarlige rådfører sig med databeskyttelsesrådgiveren, hvis en sådan er udpeget, når der foretages en konsekvensanalyse vedrørende databeskyttelse.

Denne bestemmelse har en naturlig sammenhæng med artikel 39, stk. 1, litra c, hvoraf det fremgår, at databeskyttelsesrådgiveren som minimum har til opgave at rådgive med hensyn til konsekvensanalysen og overvåge dens opfyldelse, når der anmodes herom i henhold til artikel 35.

Det følger endvidere af præambelbetragtning nr. 95, at databehandleren bør bistå den dataansvarlige, når det er nødvendigt og efter anmodning, med at sikre overholdelse af de forpligtelser, der udspringer af konsekvensanalyser vedrørende databeskyttelse og forudgående høring af tilsynsmyndigheden.

5.13.3.3. Databeskyttelsesforordningens artikel 35, stk. 3
Det fremgår af artikel 35, stk. 3, at en konsekvensanalyse vedrørende databeskyttelse, *navnlig* er påkrævet i følgende tilfælde:

a) en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person

b) behandling i stort omfang af særlige kategorier af personoplysninger, jf. artikel 9, stk. 1, eller af personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10, eller

c) systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Det fremgår bl.a. af præambelbetragtning nr. 91, at [det især vil være relevant inden behandlingen at foretage en konsekvensanalyse] i forbindelse med omfattende behandlings-

aktiviteter til behandling af meget store mængder personoplysninger på *regionalt*, *nationalt* eller *overnationalt* plan, der kan berøre mange registrerede, og som sandsynligvis vil indebære en høj risiko, f.eks. på grund af behandlingsaktiviteternes følsomhed, hvis der i overensstemmelse med det opnåede niveau af teknologisk viden sker omfattende brug af ny eller innovativ brug af teknologi, samt i forbindelse med andre behandlingsaktiviteter, der indebærer en høj risiko for registreredes rettigheder og frihedsrettigheder, navnlig hvis disse aktiviteter gør det vanskeligere for registrerede at udøve deres rettigheder.

I denne forbindelse må "regionalt" forstås sådan, at det dækker over behandlingsaktiviteter i dele af Danmark, at "nationalt" dækker over behandlingsaktiviteter i hele Danmark, og at "overnationalt" dækker over internationale behandlingsaktiviteter, herunder europæiske.

Det fremgår derudover bl.a. af præambelbetragtning nr. 91, at der også bør foretages en konsekvensanalyse vedrørende databeskyttelse, hvis personoplysninger behandles med det formål at træffe afgørelser vedrørende specifikke fysiske personer efter en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer baseret på *profilering* af disse oplysninger eller efter behandling af særlige kategorier af personoplysninger, biometriske data eller oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger.

Endvidere følger det af samme betragtning, at en konsekvensanalyse vedrørende databeskyttelse ligeledes er påkrævet ved omfattende overvågning af offentligt tilgængelige områder, navnlig ved brug af optoelektronisk udstyr, eller ved alle andre aktiviteter, hvor den kompetente tilsynsmyndighed mener, at den pågældende behandling sandsynligvis indebærer en høj risiko for registreredes rettigheder og frihedsrettigheder, navnlig fordi den hindrer registrerede i at udøve en rettighed eller gøre brug af en tjeneste eller en kontrakt, eller fordi den foretages på systematisk og omfattende vis.

Præambelbetragtning nr. 91 angiver endelig, at behandling af personoplysninger ikke bør anses for at være omfattende, hvis der er tale om en læges, sundhedspersonales eller en advokats behandling af personoplysninger om patienter eller klienter. I sådanne tilfælde bør en konsekvensanalyse vedrørende databeskyttelse ikke være obligatorisk.

Artikel 35, stk. 3, giver således en række eksempler på, hvornår det *navnlig* må antages, at en type behandling sandsynligvis vil indebære en høj risiko. Derudover bidrager præambelbetragtning nr. 91 med en fastlæggelse af det omfang en behandling skal have, før det er påkrævet af foretage en konsekvensanalyse. Eksemplerne i artikel 35, stk. 3, og i præambelbetragtning nr. 91 kan med brugen af "navnlig" ikke anses for udtømmende. De angiver

dog en rettesnor for, hvor omfattende, i hvor stort omfang eller hvor systematisk en behandling skal være, før en konsekvensanalyse er påkrævet.

Det må antages, at en behandling, der indeholder to eller flere af de elementer, der oplistes i artikel 35, stk. 3, og i præambelbetragtning nr. 75 og 91, i højere grad vil kunne medføre en høj risiko, der kræver udarbejdelse af en konsekvensanalyse efter artikel 35, stk. 1. Dette må f.eks. antages at være tilfældet, hvis en behandling både er systematisk og involverer en ny eller innovativ brug af teknologi.

Karakteren af de eksempler, der nævnes i artikel 35, stk. 3, og i præambelbetragtning nr. 91, taler ligesom artikel 35, stk. 1, dog generelt for, at området for, hvornår en konsekvensanalyse er påkrævet er snævert. Den dataansvarlige vil således i de fleste tilfælde ikke skulle foretage en konsekvensanalyse.

Af artikel 35, stk. 4, fremgår det bl.a., at tilsynsmyndigheden udarbejder og offentliggør en liste over de typer af behandlingsaktiviteter, der er underlagt kravet om konsekvensanalyse vedrørende databeskyttelse i henhold til stk. 1. Af stk. 5 fremgår det bl.a., at tilsynsmyndigheden også kan udarbejde en liste over de typer af behandlingsaktiviteter, for hvilke der ikke kræves nogen konsekvensanalyse vedrørende databeskyttelse

Det bemærkes, at hvis udfaldet af en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen *vil føre* til høj risiko, som den dataansvarlige *ikke* kan begrænse ved passende foranstaltninger, indtræder der en pligt for den dataansvarlige til at høre tilsynsmyndigheden efter forordningens artikel 36, stk. 1.

Det bemærkes endvidere, at en databehandler som følge af kravene til en databehandleraftale i medfør af artikel 28, stk. 3, litra f, skal bistå den dataansvarlige med sin forpligtelse til at udarbejde konsekvensanalyser vedrørende databeskyttelse i medfør af artikel 35.

5.13.3.4. Databeskyttelsesforordningens artikel 35, stk. 7
Det fremgår af artikel 35, stk. 7, at en konsekvensanalyse *mindst* skal omfatte:

a) en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige,

b) en vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene,

c) en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1, og

d) de foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af denne forordning, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

Litra a må fortolkes således, at der skal ske en systematisk beskrivelse af de forskellige former for behandling, som personoplysningerne vil blive genstand for. Personoplysningerne, som skal behandles, skal også være klart beskrevet og defineret. Dette gælder også i forhold til oplysninger omfattet af artikel 9 og 10. Endvidere skal en konsekvensanalyse indeholde en beskrivelse af formålet med behandlingen, herunder dataansvarliges legitime interesser. Det kan eksempelvis være behandling af personoplysninger, som enten har hjemmel i lov, eller som skal ske som led i offentlig myndighedsudøvelse.

Litra b kræver, at der foretages en vurdering af nødvendigheden af de planlagte behandlinger, og om de står i rimeligt forhold til formålene med behandlingen. Der er således tale om en bestemmelse, som blandt andet har til formål at hindre dataophobning og blandt andet også sikre, at der kun behandles personoplysninger, der er nødvendige, og som kan rummes inden for formålene med behandlingen. Behandlingen af personoplysninger må dermed ikke gå videre, end hvad der kræves for at opfylde de formål, som den dataansvarlige er berettiget til at forfølge.

Litra c kræver en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder, som omhandlet i stk. 1. Det betyder, at de registreredes rettigheder og frihedsrettigheder skal vurderes i forhold til den planlagte behandling og formålet med denne. Litra d bør læses i sammenhæng med litra c, således at der kræves en vurdering af de foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af forordningen og dansk lovgivning i øvrigt, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

Der kan i et vist omfang konstateres sammenfald mellem en række af de oplysninger, som skal indgå i de fortegnelser over behandlingsaktiviteter, som den dataansvarlige skal føre i medfør af forordningens artikel 30, og det som en konsekvensanalyse mindst skal omfatte i medfør af forordningens artikel 35, stk. 7. Hvis en dataansvarlig forpligtes til at udarbejde en konsekvensanalyse, vil de fortegnelser over behandlingsaktiviteter, som den dataansvarlige fører, i vidt omfang kunne genanvendes ved udarbejdelsen af konsekvensanalysen.

Der stilles f.eks. både krav om angivelse af formålene med behandlingen i artikel 30, stk. 2, litra b, og artikel 35, stk. 7, litra a. Derudover vil en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger i medfør af artikel 30. stk. 2, litra g, kunne anvendes i udarbejdelsen af den del af konsekvensanalysen, der bl.a. vedrører sikkerhedsforanstaltninger, jf. artikel 35, stk. 7, litra d.

I forhold til udarbejdelse af konsekvensanalyse vedrørende databeskyttelse, kan der henvises til den internationale standard ISO 29134 omhandlende "Privacy Impact Assessment" (konsekvensanalyse vedrørende privatliv). Ved at benytte denne standard kan den dataansvarlige øge sandsynligheden for at afdække væsentlige elementer i sin databehandling og samtidig få vejledning i processen og rapporteringen. Denne standard kan anvendes af både offentlige myndigheder og private virksomheder.

5.13.3.5. Databeskyttelsesforordningens artikel 35, stk. 8

Det følger af artikel 35, stk. 8, at overholdelse af godkendte adfærdskodekser, jf. artikel 40, inddrages behørigt ved vurderingen af konsekvenserne af de behandlingsaktiviteter, der udføres af de pågældende dataansvarlige eller databehandlere, navnlig i forbindelse med en konsekvensanalyse vedrørende databeskyttelse.

5.13.3.6. Databeskyttelsesforordningens artikel 35, stk. 9

Det følger af artikel 35, stk. 9, at den dataansvarlige, hvis det er *relevant*, indhenter de registreredes eller deres repræsentanters synspunkter vedrørende den planlagte behandling, uden at det berører beskyttelse af kommercielle eller samfundsmæssige interesser eller behandlingsaktiviteternes sikkerhed.

Brugen af ordet "relevant", jf. ovenfor, indikerer, at der bør foretages en konkret vurdering af risiciene for de registrerede, hver gang der skal foretages en behandling. Der er ikke tale om, at der skal foretages en konsultation af de registrerede i forbindelse med alle konsekvensanalyser, men der skal foretages en konkret vurdering af, om der er anledning til at konsultere de registrerede i forbindelse med udarbejdelsen af konsekvensanalysen.

Eksempelvis kan det være relevant, at den dataansvarlige indhenter de registreredes eller deres repræsentanters synspunkter vedrørende en planlagt behandling i forbindelse med høringsprocessen ved udarbejdelse af lovforslag mv.

Bestemmelsen må herudover forventes at få begrænset virkning i praksis.

5.13.3.7. Databeskyttelsesforordningens artikel 35, stk. 10
Det fremgår af forordningens artikel 35, stk. 10, at hvis en behandling i henhold til artikel 6, stk. 1, litra c, om behandling som er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, eller stk. 1 litra e, om behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, har et retsgrundlag i EU-retten eller i den medlemsstats nationale ret, som den dataansvarlige er underlagt, og denne ret regulerer den eller de pågældende specifikke behandlingsaktiviteter, og der allerede er foretaget en konsekvensanalyse vedrørende databeskyttelse som led i en generel konsekvensanalyse i forbindelse med vedtagelse af dette retsgrundlag, finder artikel 35, stk. 1-7, ikke anvendelse, medmindre medlemsstaterne anser det for nødvendigt at foretage en sådan analyse inden behandlingsaktiviteter.

I praksis vil en *generel* konsekvensanalyse efter artikel 35, stk. 10, kunne foretages i forbindelse med udformningen af lovforslag.

Det bemærkes, at det ikke er et krav i artikel 35, at den dataansvarlige udarbejder konksekvensanalyse i forhold til allerede eksisterende systemer i forbindelse med forordningens ikrafttrædelse, medmindre risikobilledet efter den 25. maj 2018 for de igangværende behandlingsaktiviteter efter en konkret vurdering ændrer sig.

Det er i øvrigt alene relevant at overveje undtagelsesmuligheden i artikel 35, stk. 10, i det omfang, der ellers er pligt til at udarbejde en konsekvensanalyse efter artikel 35, stk. 1.

5.13.3.8. Databeskyttelsesforordningens artikel 35, stk. 11
Det fremgår af artikel 35, stk. 11, at den dataansvarlige, hvis det er nødvendigt, foretager en fornyet gennemgang for at vurdere, hvorvidt behandling er foretaget i overensstemmelse med konsekvensanalysen vedrørende databeskyttelse. Dette gælder i hvert fald, når der er en ændring af den risiko, som behandlingsaktiviteterne udgør.

Hvis behandlingsaktiviteternes risiko ændres, eller det af anden grund vurderes nødvendigt, skal den dataansvarlige foretage en gennemgang af ændringer med henblik på at vurdere, hvorvidt behandlingen er foretaget i overensstemmelse med den oprindelige konsekvensanalyse. Dette skal på baggrund af ordlyden "i hvert fald" ske i de tilfælde, hvor der sker en ændring af den risiko, som behandlingsaktiviteterne udgør.

Det må efter bestemmelsen også være påkrævet med en fornyet konsekvensanalyse i andre situationer. Det må eksempelvis skulle vurderes, om der er behov for en fornyet gennemgang, når der sker ændringer, som betyder, at formålet med behandlingen ændres. Endvide-

re vil dette skulle ske, hvis behandlingen ændres, således at der fremover skal behandles andre personoplysninger end dem, som aktuelt bliver behandlet, herunder hvis der fremover skal behandles personoplysninger, som er omfattet af en anden kategori af personoplysninger. Dette kunne eksempelvis være, hvis et system, der omfatter behandlingsaktiviteter af personoplysninger efter artikel 9, ændres, således at der fremover skal ske behandling af personoplysninger omfattet af artikel 10. Derudover kunne det være tilfældet, hvis et eksisterende system, der behandler oplysninger efter artikel 6, udvides til også at behandle oplysninger efter artikel 9.

5.13.3.9. Tilsynsmyndighedens lister, artikel 35, stk. 4-6

Efter forordningens artikel 35, stk. 4, er der krav om, at tilsynsmyndigheden udarbejder og offentliggør en liste over behandlingsaktiviteter, der er underlagt krav om konsekvensanalyse i henhold til artikel 35, stk.1. Efter forordningens artikel 35, stk. 5, kan tilsynsmyndigheden også udarbejde og offentliggøre en liste over behandlingsaktiviteter, for hvilke der *ikke* kræves konsekvensanalyse. Tilsynsmyndigheden skal indgive de lister, den udarbejder i henhold til forordningens artikel 35, stk. 4 og 5, til Databeskyttelsesrådet.

Det følger endvidere af forordningens artikel 35, stk. 6, at tilsynsmyndigheden inden vedtagelsen af listerne skal anvende sammenhængsmekanismen i artikel 63, hvis sådanne lister omfatter behandlingsaktiviteter, der vedrører udbud af varer eller tjenesteydelser til registrerede eller overvågning af sådanne registreredes adfærd i flere medlemsstater, eller som i væsentlig grad kan påvirke den frie udveksling af personoplysninger i Unionen. I forhold til lister over behandlingsaktiviteter, for hvilke der kræves konsekvensanalyse, fremgår det af forordningens artikel 64, at Databeskyttelsesrådet afgiver en udtalelse (artikel 64, stk. 1, litra a).

Databeskyttelsesrådet afgiver ifølge forordningens artikel 64, stk. 3, udtalelse om det spørgsmål, som det har fået forelagt, forudsat at det ikke allerede har afgivet en udtalelse om samme spørgsmål. Denne udtalelse vedtages inden for otte uger med simpelt flertal. Denne frist kan forlænges med yderligere seks uger under hensyntagen til spørgsmålets kompleksitet. Databeskyttelsesrådets udtalelse om spørgsmål kan omhandle de tilfælde, der er omtalt i artikel 64, stk. 1, herunder vedtagelse af en liste over typer af behandlingsaktiviteter, som er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse.

Det følger endvidere af forordningens artikel 64, stk. 7, at den hørende tilsynsmyndighed tager videst muligt hensyn til Databeskyttelsesrådets udtalelse og senest to uger efter modtagelsen af udtalelsen giver formanden for Databeskyttelsesrådet elektronisk meddelelse om, hvorvidt den agter at fastholde eller ændre sit udkast til afgørelse, og forelægger i givet fald det ændrede udkast til afgørelse i et standardformat.

Endvidere indeholder forordningens artikel 64, stk. 8, en regel om, at artikel 65, stk. 1, om tvistbilæggelse finder anvendelse, hvis den berørte tilsynsmyndighed helt eller delvist ikke agter at følge udtalelsen fra Databeskyttelsesrådet og giver en relevant begrundelse herfor, indenfor en nærmere beskrevet frist.

5.13.4. Overvejelser

Konsekvensanalyser er ikke reguleret i gældende ret, men er blevet anbefalet af Datatilsynet i specifikke situationer og gennem vejledninger fra Digitaliseringsstyrelsen.

Det er derfor en udvidelse af gældende ret, at forordningens artikel 35 i visse tilfælde kræver udarbejdelse af en konsekvensanalyse med et nærmere bestemt minimumsindhold.

Forordningens artikel 35, stk. 1, fastlægger, at den dataansvarlige, i de tilfælde, hvor en type behandling *sandsynligvis* vil indebære en *høj risiko* for fysiske personers rettigheder og frihedsrettigheder, er forpligtet til at foretage en konsekvensanalyse. Forordningens artikel 35, stk. 3, angiver en ikke udtømmende oplistning af eksempler, hvor en konsekvensanalyse som omhandlet i stk. 1, navnlig er påkrævet.

Det kan ud fra karakteren af de eksempler, der nævnes i artikel 35, stk. 3, og i præambelbetragtning nr. 91 – med henvisningen til "meget store mængder personoplysninger på regionalt, nationalt eller overnationalt plan" – samt ud fra ordlyden af artikel 35, stk. 1, konstateres, at området for, hvornår en konsekvensanalyse er påkrævet er snævert. Dataansvarlige må således i de fleste tilfælde antages ikke at skulle udarbejde en konsekvensanalyse.

Såfremt en konsekvensanalyse er påkrævet, angiver forordningens artikel 35, stk. 7, hvad en sådan analyse mindst skal omfatte.

For så vidt angår artikel 35, stk. 10, kan det bemærkes, at som det nærmere er beskrevet i afsnit 3.4. om artikel 6, stk. 2-3, kan medlemsstaterne i medfør af artikel 6, stk. 2, opretholde eller indføre mere specifikke bestemmelser for at tilpasse anvendelsen af forordningens bestemmelser om behandling med henblik på overholdelse af artikel 6, stk. 1, litra c og e, ved at fastsætte mere præcist specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling mv.

I de tilfælde, hvor persondatabehandling finder sted på grundlag af sådanne regler fastsat i EU-retten eller i medlemsstaternes nationale ret, og der i forbindelse med gennemførelse af den pågældende lovgivning er foretaget en *generel* konsekvensanalyse vedrørende databeskyttelse, følger det således af forordningens artikel 35, stk. 10, at det ikke i forhold til den *enkelte* persondatabehandling er nødvendigt at foretage en konsekvensanalyse.

Medlemsstaterne har imidlertid mulighed for – uanset at den eller de pågældende specifikke behandlingsaktiviteter er reguleret, og at der i forbindelse med gennemførelsen af reguleringen *er* foretaget en generel konsekvensanalyse – at beslutte, at der desuagtet skal foretages en konsekvensanalyse i forhold til den enkelte persondatabehandling, jf. artikel 35, stk. 10.

Endelig følger det af artikel 35, stk. 11, at den dataansvarlige i visse tilfælde forpligtes til at foretage en fornyet gennemgang af, om en behandling er foretaget i overensstemmelse med en konsekvensanalyse.

5.13.4.1. Tilsynsmyndighedens lister

For så vidt angår forordningens artikel 35, stk. 4, kan det bemærkes, at såvel en liste over typer af behandlingsaktiviteter, der er underlagt krav om konsekvensanalyse, som en liste over typer af behandlingsaktiviteter, for hvilke der *ikke* kræves konsekvensanalyse, kan være en hjælp til de dataansvarlige ved deres vurdering af, om en konsekvensanalyse vedrørende databeskyttelse skal foretages. Begge lister må desuden antages at gøre det lettere for tilsynsmyndigheden at administrere ordningen.

Det må forventes, at der, når forordningen har fundet anvendelse i en periode, eventuelt kan opbygges yderligere viden og forståelse blandt andet via de udtalelser, som Databeskyttelsesrådet i henhold til forordningens artikel 64, stk. 1, litra a, skal afgive, når en tilsynsmyndighed har til hensigt at vedtage en liste over typer af behandlingsaktiviteter, som er underlagt kravet om konsekvensanalyse vedrørende databeskyttelse i henhold til artikel 35, stk. 4.

5.13.4.2. Tidshorisont

Forordningen angiver ikke tidsfrister for, hvornår tilsynsmyndighedens liste(r) skal foreligge. Af hensyn til listens/listernes funktion vil det være hensigtsmæssigt, at de foreligger snarest efter forordningens anvendelsestidspunkt. Som beskrevet ovenfor skal der ske forelæggelse for Databeskyttelsesrådet.

Indtil tilsynsmyndighedens liste(r) foreligger i endelig form, må de dataansvarlige vurdere behovet for konsekvensanalyse alene ud fra kriterierne i artikel 35, stk. 1-3, og de foreliggende fortolkningsbidrag, herunder præambelbetragtning 91 og eventuelle fortolkningsbidrag fra Artikel 29-gruppen eller andre.

Det kan således ikke antages, at en manglende færdiggørelse af tilsynsmyndighedens liste(r) fritager de dataansvarlige fra at foretage en konsekvensanalyse vedrørende databeskyttelse, hvis forordningen tilsiger, at dette er påkrævet.

Det må formodes, at tilsynsmyndighedens liste(r) med tiden vil blive opdateret, da det ikke er muligt på tidspunktet for listens etablering, at forudse alle relevante typer af behandlingsaktiviteter, som måtte opstå i fremtiden.

5.13.4.3. Listerne er nationale

Ifølge forordningen skal de enkelte tilsynsmyndigheder vedtage egne lister. Efter forordningen er der således ikke tale om en fælles liste for alle medlemsstater. Et betydeligt sammenfald mellem listerne vil være naturligt, men det kan ikke udelukkes, at der også kan være forskelle mellem listerne.

Den høje grad af digitalisering i Danmark eller andre særlige danske forhold kan eventuelt indebære, at særlige behandlingsaktiviteter finder sted her, som ikke er udbredte/kendte i andre medlemsstater. Hvis særlige danske behandlingsaktiviteter opfylder kriterierne for krav om konsekvensanalyse, må det således antages, at disse kunne anføres på den danske tilsynsmyndigheds liste, selv om andre landes lister ikke indeholder tilsvarende behandlingsaktiviteter. Tilsvarende må antages for udelukkelseslisten.

5.13.4.4. Listerne er ikke udtømmende

Tilsynsmyndighedens liste over, hvilke behandlingsaktiviteter der er underlagt krav om konsekvensanalyse, vil være en hjælp til de dataansvarlige ved deres vurdering af, om en konsekvensanalyse skal foretages, og vil for de behandlingsaktiviteter, der optages på listerne, være afgørende for, om der er krav om konsekvensanalyse vedrørende databeskyttelse eller ej.

Det kan imidlertid ikke antages, at listerne vil gøre udtømmende op med alle nutidige og fremtidige databehandlingssituationer. Der kan derfor fortsat være behov for, at den dataansvarlige foretager sin egen vurdering ud fra bestemmelserne i artikel 35, stk. 1-3, under inddragelse af eksemplerne i præambelbetragtning nr. 91 og eventuelle andre fortolkningsbidrag, som måtte foreligge på tidspunktet for vurderingen.

En eventuel liste fra tilsynsmyndigheden over de typer af behandlingsaktiviteter, for hvilke der *ikke* kræves konsekvensanalyse vedrørende databeskyttelse, vil ligeledes være en hjælp til de dataansvarlige. Også for denne liste må det imidlertid antages, at angivelsen af behandlingsaktiviteter ikke vil være udtømmende, og at der fortsat vil være behov for, at den dataansvarlige foretager sin egen vurdering.

De(n) vedtagne liste(r) kan udelukkende anses som en hjælp til at vurdere, om en behandlingsaktivitet er omfattet af kravet om konsekvensanalyse eller ej. Andre bestemmelser i

forordningen kan ikke formodes/vurderes efterlevet ud fra informationen i tilsynsmyndighedens liste(r).

Det må antages, at hvis en databehandlingsaktivitet er angivet på tilsynsmyndighedens liste over behandlingsaktiviteter, for hvilke der *ikke* kræves konsekvensanalyse vedrørende databeskyttelse (såfremt en sådan laves), kan den dataansvarlige undlade at udføre en konsekvensanalyse efter artikel 35.

5.13.4.5. Ajourføring af listerne
Det må antages, at ajourføring af listerne skal ske under iagttagelse af den samme procedure som ved den oprindelige udarbejdelse.

5.14. Høring af tilsynsmyndigheden, artikel 36

5.14.1. Præsentation
I tilknytning til kravet om konsekvensanalyse vedrørende databeskyttelse kræver databeskyttelsesforordningen ved visse behandlinger, at tilsynsmyndigheden høres, før behandlingen påbegyndes.

5.14.2. Gældende ret
Persondatalovens kapitel 12-15 indeholder krav om, at visse behandlinger skal anmeldes til Datatilsynet eller Domstolsstyrelsen, og i en række tilfælde skal der også indhentes en forudgående udtalelse eller tilladelse fra tilsynsmyndigheden.

Persondataloven indeholder en række undtagelser fra kravet om anmeldelse og yderligere undtagelser er fastsat i bekendtgørelserne om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning (bekendtgørelse nr. 529 af 15. juni 2000), bekendtgørelsen om undtagelse fra pligten til anmeldelse af visse behandlinger, der foretages for domstolene (bekendtgørelse nr. 532 af 15. juni 2010) og bekendtgørelsen om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for en privat dataansvarlig (bekendtgørelse nr. 534 af 15. juni 2000). Dette indebærer samtidig, at der ved disse behandlinger ikke er krav om forudgående udtalelse/tilladelse fra Datatilsynet eller Domstolsstyrelsen.

En anmeldelse til Datatilsynet har ikke betydning for de materielle betingelser for behandlingen af personoplysninger. Det er således den dataansvarliges eget ansvar at vurdere, om en behandling – herunder indsamling, registrering og videregivelse – kan ske i overensstemmelse med persondataloven. Der er med andre ord ikke tale om, at en udtalelse eller

tilladelse fra Datatilsynet på forhånd gør op med eller godkender alle fremtidige databehandlinger, der vil ske hos den dataansvarlige som led i de anmeldte behandlingsaktiviteter.

Datatilsynet skal give tilladelse til behandling eller videregivelse af visse typer af personoplysninger (persondatalovens §§ 7, 10, 13, 19 og 27).

I forbindelse med visse behandlingsaktiviteter har Datatilsynet desuden mulighed for at stille vilkår, herunder som led i tilladelser.

I anmeldelser fra offentlige myndigheder skal de dataansvarlige angive i anmeldelsen, hvorvidt relevante kapitler i sikkerhedsbekendtgørelsen vil blive efterlevet.

I anmeldelser fra private virksomheder vil der som oftest medfølge en kortfattet beskrivelse af de sikkerhedsforanstaltninger, der vil blive truffet. Datatilsynet vil derefter eventuelt følge op med vilkår om bl.a. datasikkerhed i sin tilladelse.

Angående krav om høring i forbindelse med ny lovgivning fremgår det af persondatalovens § 57, at der ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger, skal indhentes en udtalelse fra Datatilsynet.

Af bemærkningerne til persondataloven fremgår det bl.a., at Datatilsynet i forbindelse med høringerne skal udtale sig om, hvorvidt påtænkte retsforskrifter mv. efter tilsynets opfattelse giver anledning til betænkeligheder i forhold til databeskyttelsesdirektivet og persondataloven eller i øvrigt i relation til beskyttelsen af de registreredes privatliv.

Selv ved vejledninger kan det være relevant at følge § 57, idet en vejledning kan være et vigtigt styremiddel.[619] Datatilsynet har gennem årene fået en del vejledninger i høring og har i en række tilfælde afgivet bemærkninger.

5.14.3. Databeskyttelsesforordningen

Efter forordningens artikel 36, stk. 1, skal den dataansvarlige høre tilsynsmyndigheden inden behandling, *hvis* en konsekvensanalyse vedrørende databeskyttelse foretaget i henhold til artikel 35 viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen. Artikel 36, stk. 1, angiver ikke præcist, hvad der menes med "høj risiko", men det kan formodes, at der er tale om den type høj

[619] Persondataloven med kommentarer (2015), s. 624.

risiko, som er nævnt i artikel 35 stk. 1, nemlig "høj risiko for fysiske personers rettigheder og frihedsrettigheder".

Det fremgår endvidere af forordningens artikel 36, stk. 2, at hvis tilsynsmyndigheden finder, at den planlagte behandling omhandlet i stk. 1 overtræder denne forordning, navnlig hvis den dataansvarlige ikke tilstrækkeligt har identificeret eller begrænset risikoen, skal tilsynsmyndigheden inden for en periode på op til otte uger efter modtagelse af anmodningen om høring give den dataansvarlige, og hvor det er relevant, databehandleren skriftlig rådgivning og kan i den forbindelse anvende enhver af sine beføjelser, jf. artikel 58. Denne periode kan forlænges med seks uger under hensyntagen til den påtænkte behandlings kompleksitet. Tilsynsmyndigheden underretter den dataansvarlige, og, hvor det er relevant, databehandleren om enhver sådan forlængelse senest en måned efter modtagelse af anmodningen om høring sammen med begrundelsen for forsinkelsen. Disse perioder kan suspenderes, indtil tilsynsmyndigheden har modtaget oplysninger, som den har anmodet om med henblik på høringen.

Herudover fremgår det af forordningens artikel 36, stk. 3, at når tilsynsmyndigheden skal høres i henhold til stk. 1, indgiver den dataansvarlige følgende til tilsynsmyndigheden:

a) hvor det er relevant, ansvarsområderne for henholdsvis den dataansvarlige, fælles dataansvarlige og databehandleren, der er involveret i behandlingen, navnlig med hensyn til behandling inden for en koncern
b) den planlagte behandlings formål og hjælpemidler
c) foranstaltninger og garantier til beskyttelse af de registreredes rettigheder og frihedsrettigheder i henhold til denne forordning
d) hvor det er relevant, databeskyttelsesrådgiverens kontaktoplysninger
e) konsekvensanalysen vedrørende databeskyttelse i henhold til artikel 35, og
f) andre oplysninger, som tilsynsmyndigheden anmoder om.

Af præambelbetragtning nr. 84 fremgår bl.a, at hvis det fremgår af en konsekvensanalyse vedrørende databeskyttelse, at behandlingsaktiviteter indebærer en høj risiko, som den dataansvarlige ikke kan begrænse ved passende foranstaltninger med hensyn til tilgængelig teknologi og gennemførelsesomkostninger, bør tilsynsmyndigheden høres forud for behandlingen.

Når præambelbetragtning nr. 84 omtaler "en høj risiko", er der tale om det, som forordningen i andre sammenhænge omtaler som "en høj risiko for fysiske personers rettigheder og frihedsrettigheder". Dette understøttes af, at der i præambelbetragtning nr. 84 hentydes til resultatet af en konsekvensanalyse vedrørende databeskyttelse, og disse konsekvensanaly-

ser skal ifølge artikel 35, stk. 1, foretages, når en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

Præambelbetragtning nr. 89 angiver, at der ved databeskyttelsesdirektivet blev fastsat en generel forpligtelse til at anmelde behandlingen af personoplysninger til tilsynsmyndighederne. Denne forpligtelse medførte en administrativ og finansiel byrde, men den bidrog ikke i alle tilfælde til at forbedre beskyttelsen af personoplysninger. En sådan vilkårlig og generel anmeldelsespligt bør derfor afskaffes og erstattes med effektive procedurer og mekanismer, som i stedet fokuserer på de typer behandlingsaktiviteter, der sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder i medfør af deres karakter, omfang, sammenhæng og formål. Sådanne typer behandlingsaktiviteter kan være aktiviteter, der navnlig indebærer brug af ny teknologi, eller aktiviteter som er af en ny slags, og hvor den dataansvarlige endnu ikke har foretaget en konsekvensanalyse vedrørende databeskyttelse, eller hvor de er blevet nødvendige på grund af den tid, der er gået siden den oprindelige behandling.

Præambelbetragtning nr. 94 angiver, at såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at en behandling uden garantier, sikkerhedsforanstaltninger og mekanismer til at begrænse risikoen vil føre til en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og den dataansvarlige mener, at risikoen ikke kan begrænses gennem rimelige midler for så vidt angår tilgængelig teknologi og gennemførelsesomkostninger, bør tilsynsmyndigheden høres inden indledning af behandlingsaktiviteterne. En sådan høj risiko vil sandsynligvis være en følge af visse typer behandling samt omfanget og hyppigheden af behandlingen, der også kan føre til skade for eller indgreb i fysiske personers rettigheder og frihedsrettigheder. Tilsynsmyndigheden bør reagere på en høringsanmodning inden for et fastsat tidsrum. Tilsynsmyndighedens manglende reaktion inden for dette tidsrum bør dog ikke berøre tilsynsmyndighedens mulighed for at gribe ind i overensstemmelse med dens opgaver og beføjelser i henhold til denne forordning, herunder beføjelsen til at forbyde behandlingsaktiviteter. Som led i denne høringsproces kan resultatet af en konsekvensanalyse vedrørende databeskyttelse, der foretages for den pågældende behandling, forelægges tilsynsmyndigheden, navnlig de foranstaltninger, der påtænkes for at begrænse risikoen for fysiske personers rettigheder og frihedsrettigheder.

Efter forordningens artikel 36, stk. 4, hører medlemsstaterne tilsynsmyndigheden som led i udarbejdelse af et forslag til lovgivningsmæssige foranstaltninger, som skal vedtages af et nationalt parlament, eller af en regulerende foranstaltning, der har hjemmel i en sådan lovgivningsmæssig foranstaltning, som vedrører behandling.

Det fremgår endvidere af forordningens artikel 36, stk. 5, at uanset stk. 1 kan det i medlemsstaternes nationale ret kræves, at dataansvarlige hører og opnår forudgående tilladelse fra tilsynsmyndigheden i forbindelse med en dataansvarligs behandling under udførelsen af en opgave i samfundets interesse, herunder behandling i forbindelse med social sikring og folkesundhed.

Om den forudgående høring i forbindelse med lovgivningsmæssige foranstaltninger fremgår det af præambelbetragtning nr. 96, at tilsynsmyndigheden ligeledes bør høres som led i udarbejdelsen af lovgivning eller regulerende foranstaltninger, som omhandler behandling af personoplysninger, med henblik på at sikre, at den planlagte behandling overholder forordningen, og navnlig for at begrænse risiciene for den registrerede.

5.14.3.1. Muligheden for at indføre krav om forudgående høring og tilladelse fra tilsynsmyndigheden, artikel 36, stk. 5

Som det nærmere er beskrevet i afsnit 5.7. om fortegnelseskravet i artikel 30, følger det af databeskyttelsesdirektivets artikel 18, stk. 1, og persondatalovens §§ 43, stk. 1 og 48, at der i visse situationer skal ske anmeldelse til Datatilsynet, og at denne anmeldelse skal indeholde en optegnelse over de behandlingsaktiviteter, der anmeldes. Det fremgår af persondatalovens §§ 45 og 50, at der skal indhentes udtalelse eller tilladelse fra Datatilsynet, forinden en behandling, der er omfattet af anmeldelsespligten, iværksættes.

Databeskyttelsesforordningens artikel 30 lægger op til en anden ordning end efter anmeldelsesordningen i gældende ret, hvorefter den dataansvarlige og databehandleren i visse tilfælde skal føre fortegnelser over deres behandling af personoplysninger, hvilket ligger fint i tråd med forordningens risikobaserede tilgang og fokus på ansvarlighed ("accountability").

Forordningen giver som nævnt for så vidt angår behandling *under udførelse af en opgave i samfundets interesse* dog mulighed for, at medlemsstaterne i national ret *generelt* kan kræve, at den dataansvarlige hører og opnår forudgående tilladelse fra tilsynsmyndigheden, også i de tilfælde, som ellers ikke er omfattet af kravet om forudgående høring af tilsynsmyndigheden, jf. artikel 36, stk. 1.

Forordningens artikel 36, skt. 5, åbner således op for, at medlemsstaterne kan fastsætte nærmere regler om, at den dataansvarlige i forbindelse med visse behandlingsaktiviteter *altid* – uanset om konsekvensanalysen har vist, at behandlingen vil medføre en høj risiko i mangel af foranstaltninger eller ej – skal høre og opnå forudgående tilladelse fra tilsynsmyndigheden – altså en fravigelse af forordningens udgangspunkt om en afskaffelse af anmeldelseskrav.

Denne fravigelse af forordningens almindelige ordning, som artikel 36, stk. 5, giver rum for, er dog begrænset til behandlingsaktiviteter som led i "udførelse af en opgave i samfundets interesse". Som eksempler herpå nævner forordningen behandling i forbindelse med social sikring og folkesundhed.

Et specifikt *eksempel* på en behandling under udførelse af en opgave i samfundet interesse, som må antages at kunne rummes inden for rammerne af artikel 36, stk. 5, er behandling til historiske og videnskabelige forskningsformål og statistiske formål. Det må derfor antages, at ordningen i persondatalovens § 10, stk. 3, om tilladelse til videregivelse af oplysninger omfattet af persondatalovens § 10, stk. 1 og 2, til tredjemand, også *kan* rummes inden for rammerne af forordningens artikel 36, stk. 5, og således opretholdes i dansk ret.

5.14.4. Overvejelser

5.14.4.1. Artikel 36, stk. 1-3

I dag findes der regler om forudgående høring af tilsynsmyndigheden i persondatalovens regler om forudgående udtalelse eller tilladelse fra Datatilsynet eller Domstolsstyrelsen i forbindelse med anmeldelser.

5.14.4.1.2. Forpligtelsen til at foretage høring

Det udslagsgivende for kravet i forordningen om høring af tilsynsmyndigheden er udfaldet på en konsekvensanalyse vedrørende databeskyttelse. Hvis analysen viser, at behandlingen ikke vil føre til høj risiko som følge af *foranstaltninger truffet af den dataansvarlige* for at begrænse risikoen, skal tilsynsmyndigheden ikke høres. Høringspligten indtræder således kun, hvis behandlingsaktiviteter indebærer en høj risiko, som den dataansvarlige *ikke* kan begrænse ved passende foranstaltninger, jf. også præambelbetragtning nr. 84.

Udtrykket "foranstaltninger" synes at være uddybet i præambelbetragtning nr. 94 som "garantier, sikkerhedsforanstaltninger og mekanismer til at begrænse risikoen". Udtrykket "garantier" er oversat fra den engelske sprogversion, fra udtrykket 'safeguards', hvilket i denne sammenhæng kan forstås som "værn" eller "beskyttelse".

Som en konsekvens af artikel 36, stk. 1, vil tilsynsmyndigheden således muligvis aldrig få kendskab til behandlingens eksistens, herunder anledning til at vurdere, om den foretagne konsekvensanalyse er retvisende.

5.14.4.1.3. Tilsynsmyndighedens reaktion

Et muligt udfald på høringen er, at tilsynsmyndigheden finder, at den planlagte behandling overtræder forordningen og skal give den dataansvarlige skriftlig rådgivning, som beskre-

vet i artikel 36, stk. 2. Der er ikke krav om skriftlig vejledning, hvis tilsynsmyndigheden *ikke* finder, at den planlagte behandling overtræder forordningen.

Overtrædelse af forordningen kan efter artikel 36, stk. 2, foreligge "navnlig, hvis den dataansvarlige ikke tilstrækkeligt har identificeret eller begrænset risikoen". Det må imidlertid antages, at tilsynsmyndigheden også skal reagere, hvis den finder, at den planlagte behandling på andre punkter overtræder forordningen.

Det kunne f.eks. være, hvis det fremsendte viser, at de påtænkte behandlingsaktiviteter går videre, end hvad der er muligt efter forordningens betingelser. Omvendt vil det ikke kunne antages, at en manglende reaktion fra tilsynsmyndigheden er udtryk for, at enhver kommende databehandling i forbindelse med den forelagte aktivitet er i overensstemmelse med forordningen, og tilsynsmyndigheden kan dermed stadig gribe ind i overensstemmelse med til sine beføjelser i henhold til forordningen (præambelbetragtning nr. 94). Som under den gældende persondatalov vil det også under forordningen være den dataansvarliges eget ansvar at vurdere, om en behandling – herunder indsamling, registrering og videregivelse – kan ske i overensstemmelse med forordningen. En udtalelse fra tilsynsmyndigheden som svar på en artikel 36-høring vil således ikke på forhånd gøre op med eller godkende alle fremtidige databehandlinger, der vil ske hos den dataansvarlige som led i de omhandlede behandlingsaktiviteter.

Selv om tilsynsmyndigheden ikke fremkommer med en tilkendegivelse om, at behandlingen overtræder forordningen, kan det således ikke betragtes som tilsynsmyndighedens "godkendelse" eller "blåstempling" af en behandlingsaktivitet.

Hvis tilsynsmyndigheden finder, at den planlagte behandling overtræder forordningen, *skal* den give skriftlig rådgivning indenfor en periode på op til otte uger og kan i den forbindelse anvende enhver af sine beføjelser. Ved brug af sine undersøgelsesbeføjelser (artikel 58, stk. 1) og gennem artikel 36, stk. 3, litra f, kan tilsynsmyndigheden f.eks. kræve at få yderligere oplysninger. Tilsynsmyndigheden kan også anvende sine korrigerende beføjelser (artikel 58, stk. 2) f.eks. til at begrænse eller forbyde en behandling. Endeligt er artikel 36-høringerne et tilfælde, hvor tilsynsmyndigheden har rådgivnings- og vejledningsbeføjelser (efter artikel 58, stk. 3).

5.14.4.1.4. Grundlaget for tilsynsmyndighedens behandling

Artikel 36, stk. 3, beskriver, hvad den dataansvarlige skal indgive til tilsynsmyndigheden i forbindelse med høringen. I den forbindelse er der også pligt til at give andre oplysninger, som tilsynsmyndigheden anmoder om (litra f), hvilket ligeledes følger af reglerne om tilsynets undersøgelsesbeføjelser.

Det kunne eksempelvis komme på tale at anmode om oplysninger om, hvor personoplysninger vil blive behandlet, herunder om dette vil ske hos databehandlere (herunder eventuelle underdatabehandlere) uden for EU, og på hvilket grundlag overførsler af oplysninger til tredjelande(t) i givet fald vil finde sted.

Såfremt tilsynsmyndigheden i sin praksis identificerer, at en given oplysningstype generelt vil være relevant at få oplyst i disse sager, vil det være hensigtsmæssigt, at tilsynet informerer herom på sin hjemmeside.

5.14.4.2. Artikel 36, stk. 4

Persondataloven angiver, at Datatilsynet skal høres ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger. Forordningen angiver at krav om høring af tilsynsmyndigheden også skal ske ved "regulerende foranstaltning".

5.14.4.3. Artikel 36, stk. 5

Persondataloven omfatter krav om forudgående anmeldelse til og tilladelse fra Datatilsynet, ved visse behandlinger. Disse krav bortfalder ved overgangen til forordningen. I forordningen er der imidlertid mulighed for, at man i national ret kan kræve, at dataansvarlige hører og opnår forudgående tilladelse fra tilsynsmyndigheden i forbindelse med en dataansvarligs behandling under udførelsen af en opgave i samfundets interesse, herunder behandling i forbindelse med social sikring og folkesundhed.

5.15. Krigsreglen

5.15.1. Præsentation

Den såkaldte "krigsregel" følger af persondatalovens § 41, stk. 4, hvoraf det fremgår, at for oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Bestemmelsen indebærer i praksis bl.a., at visse større landsdækkende administrative systemer og specialregistre ikke må føres i udlandet.[620]

Krigsreglen står i persondatalovens kapitel 11 om behandlingssikkerhed.

[620] Datatilsynets udtalelse vedrørende OCES II løsningen, brev af 3. april 2009, Datatilsynets j.nr. 2009-122-0247 og høringssvar til lovforslag om digital post af 13. februar 2012, Datatilsynets j.nr. 2012-112-0011.

Databeskyttelsesdirektivet og databeskyttelsesforordningen indeholder ikke en tilsvarende regel. Det er relevant at foretage en vurdering af, hvorvidt der i national ret, når forordningen finder anvendelse fra den 25. maj 2018, er mulighed for at opretholde den danske krigsregel eller eventuelt videreføre krigsreglen i en revideret udgave.

5.15.2. Gældende ret

Det fremgår af persondatalovens § 41, stk. 4, at der for oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Det fremgår af bemærkningerne til persondataloven, at persondatalovens § 41, stk. 4, svarer til, hvad der fulgte af lov om offentlige myndigheders registre § 12, stk. 3, og omfatter behandling af oplysninger, som en besættelsesmagt eller en magt, der har erobret en del af landet, vil have særlig interesse i bl.a. for dermed hurtigt og effektivt at kunne overtage den almindelige administration.[621]

Registerudvalget anførte således i betænkning nr. 1345, at udvalget fandt det hensigtsmæssigt i lovudkastets § 41, stk. 2, (nu persondatalovens § 41, stk. 4) at opretholde en bestemmelse om, at offentlige myndigheder skal træffe foranstaltninger, som muliggør bortskaffelse eller tilintetgørelse af oplysninger, som er af særlig interesse for fremmede magter i tilfælde af krig eller lignende forhold, jf. lov om offentlige myndigheders registre § 12, stk. 3. Udvalget anførte endvidere, at det i øvrigt følger af databeskyttelsesdirektivets artikel 3, stk. 2, 1. pind, at direktivet ikke omfatter behandlinger, som vedrører bl.a. statens sikkerhed og forsvar.[622]

Det fremgår af bemærkningerne til persondataloven, at navnlig de større landsdækkende administrative systemer, som f.eks. Det Centrale Personregister (CPR) og centrale skattesystemer, vil være omfattet af bestemmelsen. Det samme gælder specialregistre, som kan benyttes til at finde frem til bestemte personer, som den fremmede magt – eksempelvis på grund af de pågældendes særlige uddannelse – ønsker at disponere over. På samme måde vil en fremmed magt kunne have særlig interesse i at få adgang til edb-systemer mv. med oplysninger om større lastmotorkøretøjer.[623]

[621] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 41.
[622] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 327.
[623] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 41.

Det fremgår endvidere af bemærkningerne til persondataloven, at Datatilsynet vil kunne henlede opmærksomheden på behovet for særlige foranstaltninger, hvis tilsynet bliver bekendt med, at en behandling som nævnt i persondatalovens § 41, stk. 4, finder sted.[624]

Endelig følger det af bemærkningerne, at krigsreglen ikke indebærer, at de omtalte oplysninger nødvendigvis skal bortskaffes eller destrueres i tilfælde af krig eller lignende forhold. Bestemmelsen sikrer blot, at der lovligt vil kunne træffes beslutning om destruktion mv., hvis det skulle vise sig nødvendigt. Det påhviler den dataansvarlige at træffe de foranstaltninger, som muliggør destruktion mv.[625]

Bestemmelsen indebærer efter sin ordlyd heller ikke, at en bestemt given behandling nødvendigvis *skal* føres i Danmark.

Reglen i persondatalovens § 41, stk. 4, indebærer dog, at ikke alle behandlinger – offentlige eller private – vil kunne udføres af en databehandler i et andet EU-land, hvilket ellers er udgangspunktet i databeskyttelsesdirektivet, i det omfang en behandling er omfattet af direktivet. Eksempelvis antages det, at *Det Centrale Kriminalregister* og *Det Centrale Personregister* ikke må føres i udlandet.[626]

I et svar på spørgsmålene nr. 25, 27, 64 og 69 af 5. januar 1999 til Folketingets Retsudvalg ad L 44 (Folketinget 1998-1999) anførte Justitsministeriet tilsvarende, at bestemmelsen i lovforslagets § 41, stk. 2, (nu persondatalovens § 41, stk. 4), efter Justitsministeriets opfattelse indebærer, at Det Centrale Kriminalregister ikke må føres i udlandet.

Indenrigsministeriet anførte endvidere i et svar på spørgsmål nr. 6 fra Folketingets Kommunaludvalg vedrørende forslag til lov om Det Centrale Personregister (L 9), at en forudsætning for, at Indenrigsministeriet kan sikre den omhandlede bortskaffelse eller tilintetgørelse (i overensstemmelse med persondatalovens § 41, stk. 4) er, at driftsafviklingen af CPR-registret fysisk sker her i landet undergivet dansk jurisdiktion.

Som et andet eksempel i lovgivningspraksis kan nævnes CPR-lovens § 55. Af CPR-lovens § 55, stk. 1, fremgår det, at Økonomi- og Indenrigsministeriet træffer foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse af CPR i tilfælde af krig eller lignende forhold. I CPR-lovens § 55, stk. 2 – 4, er fastsat nærmere bestemmelser om administration af personregistreringen forud for en eventuel krig eller lignende forhold, om etablering af et særligt

[624] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 41.
[625] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 41.
[626] Persondataloven med kommentarer (2015), s. 555.

beredskab, der gør det muligt at udtrække oplysninger til brug for fremstilling af valglister og -kort, samt om muligheden for at pålægge bl.a. offentlige myndigheder at meddele oplysninger, som er nødvendige til CPR's genoprettelse.

Fra Datatilsynets praksis kan nævnes sagen, hvor ATP ønskede at overføre deres behandling af oplysninger til databehandlere i Indien og Sydafrika primært af hensyn til forsyningssikkerheden på grundlag af databehandlerkontrakter. ATP's behandling af oplysninger omfattede oplysninger om medlemmers navn, adresse og øvrige kontaktoplysninger, personnummer samt oplysninger om arbejdsgiver, stilling, erhverv eller uddannelse. Der var tale om behandling af oplysninger fra næsten 4,5 millioner medlemmer og godt 150.000 indbetalende arbejdsgivere, både offentlige og private. Derudover fik ATP indbetalinger fra kommuner og Arbejdsdirektoratet (A-kasser).

Datatilsynet fandt i denne sag, at den behandling af personoplysninger, som ATP og ATP's samarbejdspartnere foretog i deres almindelige systemer, var omfattet af persondatalovens § 41, stk. 4.

Datatilsynet udtalte således, at bestemmelsen i § 41, stk. 4, blev opretholdt ved Folketingets beslutning i 2000, og at en bortskaffelses- eller tilintetgørelsesadgang, der alene er baseret på aftaler herom, heller ikke i 2000 synes forudsat som en tilstrækkelig sikker løsning. ATP kunne derfor ikke benytte den ønskede løsning for behandling af oplysninger. I denne forbindelse lagde Datatilsynet navnlig vægt på, at databehandlere og dataansvarlige, der befinder sig i Danmark, er underlagt dansk lovgivning, hvilket ikke gør sig gældende for databehandlere uden for Danmark.

Datatilsynet udtalte endvidere, at tilsynet i den forbindelse måtte understrege, at tilsynet ikke fandt at kunne tage stilling til, hvorvidt den nuværende trusselssituation ændrede forudsætningerne for bestemmelsen i § 41, stk. 4, herunder om bestemmelsen fortsat burde opretholdes. Tilsynet udtalte, at dette i givet fald måtte forudsætte en politisk beslutning.[627]

5.15.3. Databeskyttelsesforordningen

Databeskyttelsesforordningens artikel 2 regulerer det materielle anvendelsesområde for forordningen.

Ifølge forordningens artikel 2, stk. 2, litra a, gælder forordningen ikke for behandling af personoplysninger under udøvelse af aktiviteter, der falder uden for EU-retten.

[627] Vedrørende spørgsmål om krigsreglen i forhold til databehandler i tredjeland af 10. maj 2007, Datatilsynets j.nr. 2007-214-0004.

Det fremgår herom af præambelbetragtning nr. 16, at forordningen ikke finder anvendelse på spørgsmål vedrørende beskyttelse af grundlæggende rettigheder og frihedsrettigheder eller fri udveksling af personoplysninger, der vedrører aktiviteter, som falder uden for EU-retten, såsom aktiviteter vedrørende *statens sikkerhed*.

Databeskyttelsesforordningen indeholder ikke nærmere fortolkningsbidrag til udtrykket "statens sikkerhed".

Som anført i afsnit 2.1. om anvendelsesområde må der skulle anlægges samme fortolkning af undtagelsen i forordningens artikel 2, stk. 2, som for databeskyttelsesdirektivets artikel 3, stk. 2, som ikke adskiller sig væsentligt fra undtagelserne i forordningen.

Registerudvalget anførte, som tidligere anført i betænkning nr. 1345, at udvalget fandt det hensigtsmæssigt at opretholde persondatalovens § 41, stk. 4. Udvalget anførte endvidere, at det i øvrigt følger af databeskyttelsesdirektivets artikel 3, stk. 2, 1. pind, at direktivet ikke omfatter behandlinger, som vedrører bl.a. statens sikkerhed og forsvar.

Registerudvalget fandt således, at det på baggrund af databeskyttelsesdirektivets anvendelsesområde var muligt at opretholde den såkaldte krigsregel. Formålet bag krigsreglen var således netop hensynet til statens sikkerhed og forsvar.

Forordningens anvendelsesområde for så vidt angår statens sikkerhed ses, som anført, at være identisk med direktivets anvendelsesområde. Dette følger også særligt af præambelbetragtning nr. 16, hvor hensynet til statens sikkerhed fremhæves som værende uden for EU-retten.

På denne baggrund må det antages, at det fortsat vil være muligt at opretholde den danske "krigsregel" eller en tilsvarende regel ved siden af forordningen, så længe hensynet bag reglen er statens sikkerhed.

Vedrørende begrebet *statens sikkerhed* anfører Peter Blume, at det faktum, at forordningen ikke finder anvendelse med henblik på statens sikkerhed først og fremmest indebærer, at forordningen ikke finder anvendelse i forhold til efterretningstjenesterne, dvs. PET og FE. Derudover er det klart, at i det omfang en anden offentlig myndighed end PET og FE foretager behandling af personoplysninger, der udelukkende tager sigte på den nationale sikkerhed, vil også denne behandling falde uden for forordningens anvendelsesområde.[628]

[628] Peter Blume, Den nye persondataret (2016), s. 50f.

Endvidere blev det eksempelvis i forbindelse med forslag til lov om Center for Cybersikkerhed i forarbejderne anført, at den samlede karakter af de opgaver, som centeret i dag løser, medfører, at centeret ikke er omfattet af databeskyttelsesdirektivet, jf. direktivets artikel 3, stk. 2, af hensyn til behandling af oplysninger vedrørende den offentlige sikkerhed, forsvar og statens sikkerhed.[629]

Det må således lægges til grund, at lovgiver, særligt på baggrund af præambelbetragtning nr. 16, vil have et nationalt råderum for at fastsætte nationale særregler under udøvelse af aktiviteter vedrørende statens sikkerhed, der falder uden EU-retten, jf. forordningens artikel 2, stk. 2, litra a. Vurderingen af, hvornår der er tale om en aktivitet vedrørende statens sikkerhed, foretages som klart udgangspunkt nationalt. Der kan i den forbindelse henses til, at det også fremgår af artikel 4, stk. 2, i EU-traktaten, at navnlig den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar. Der kan også henvises til EU-Domstolens domme i bl.a. sag C-145/09, Tsakouridis, dom af 23. november 2010, og i sag C-348/09, P.I., dom af 22. maj 2012.

På denne baggrund kan det antages, at medlemsstaterne også efter den 25. maj 2018, hvorfra databeskyttelsesforordningen finder anvendelse, vil kunne opretholde lovgivning, som vedrører statens sikkerhed og derfor falder uden for forordningens anvendelsesområde.

Det klare udgangspunkt vil derfor være, at reglen i persondatalovens § 41, stk. 4 (eller en tilsvarende bestemmelse), om, at for oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold, kan opretholdes i en ny udgave af persondataloven – i det omfang det sker af hensyn til statens sikkerhed. Dette også henset til, at reglen allerede af Registerudvalget blev vurderet som værende i overensstemmelse med databeskyttelsesdirektivet.

Det bemærkes, at det er en del af forordningens formål, at den frie udveksling af personoplysninger i Unionen hverken indskrænkes eller forbydes af grunde, *der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger*, jf. artikel 1, stk. 3. Dette formål skal dog naturligvis ikke iagttages i det omfang en behandling eller en national lovgivning falder uden for forordningens anvendelsesområde, jf. artikel 2, stk. 2, litra a.

Det bemærkes afslutningsvis, at en arbejdsgruppe bestående af Digitaliseringsstyrelsen, Justitsministeriet og Datatilsynet i 2011 afgav en rapport, som indeholdt anbefalinger til,

[629] Forslag nr. 192, FT 2013/14, fremsat 2. maj 2014 til lov om Center for Cybersikkerhed, de almindelige bemærkninger, afsnit 8.

hvilke regelændringer der kunne blive tale om at foretage, for at det offentlige i højere grad kunne få udbytte af cloud computing. Det fremgik af denne rapport vedrørende krigsreglen, at hvis en udførelse af en behandling ved en databehandler, der er etableret i et andet land, indebærer, at persondatalovens § 41, stk. 4, ikke kan iagttages, vil behandlingen ikke kunne overlades til den pågældende. Arbejdsgruppen anførte endvidere, at dette også gælder, hvis databehandleren er placeret i et andet EU-land. Arbejdsgruppen udtalte i den forbindelse, at gruppen havde overvejet, om bestemmelsen kunne udgøre et EU-retligt problem i forhold til den fri bevægelighed af cloud computing ydelser, jf. princippet om fri bevægelighed for tjenesteydelser (EUF-Traktatens artikel 56, stk. 1.). Det var dog arbejdsgruppens vurdering, at bestemmelsen ikke var i strid med EU-retten.[630]

Det fremgår endvidere af rapporten vedrørende en eventuel ophævelse af krigsreglen, at arbejdsgruppens ministeriepræsentanter anbefalede, at bestemmelsen ikke blev ændret eller ophævet, men at det blev overladt til hver enkelt minister, som har ansvaret for registre mv., der er omfattet af bestemmelsen, at tage stilling til, om der i vedkommende særlovgivning blev indsat en bestemmelse om, at § 41, stk. 4, ikke finder anvendelse på registreret mv. – f.eks. med henblik på, at registeret skal kunne føres under en ordning med cloud computing. Arbejdsgruppens ministeriepræsentanter fremhævede endvidere, at det måtte antages, at det i praksis er relativt få registre, der er omfattet af bestemmelsen i § 41, stk. 4.[631]

5.15.4. Overvejelser

Selvom en dansk "krigsregel", som nævnt ovenfor, kan opretholdes, så længe hensynet bag reglen er statens sikkerhed, er det nærliggende nærmere at overveje behovet for samt i givet fald *indretningen* af en sådan bestemmelse i dansk ret.

Der er således sket en betydelig teknologisk udvikling siden vedtagelsen af persondataloven i 2000, hvorefter den fysiske driftsafvikling af et system inden for Danmarks grænser ikke nødvendigvis længere er en garanti for at sikre bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold. Kravet om at sikre bortskaffelse eller tilintetgørelse af de oplysninger, der er indeholdt i registrene vil således *måske* kunne ske ved at anvende en anden sikkerhedsmodel.

[630] Notat om love og regler der unødigt vanskeliggør anvendelsen af cloud computing fra Digitaliseringsstyrelsen, pkt. 4.6.
[631] Notat om love og regler der unødigt vanskeliggør anvendelsen af cloud computing fra Digitaliseringsstyrelsen, pkt. 6.6.

5.16. Cloud computing

5.16.1. Præsentation

Gennemførelsen af outsourcing ved brug af cloud computing er genstand for stor offentlig interesse på såvel europæisk som nationalt plan i kraft af muligheden for at opnå bl.a. omkostningsreduktioner, højere effektivitet og øget fleksibilitet i virksomheder og myndigheders opgavevaretagelse.

Cloud computing-løsninger anvendes i stor udstrækning af private virksomheder og privatpersoner, mens det ikke i en dansk sammenhæng har været anvendt i større udstrækning af offentlige myndigheder. Cloud computing er imidlertid medtaget i den fællesoffentlige digitaliseringsstrategi 2016-2020 – som fokusområde 4, hvor det bl.a. fremgår, at "*[d]en offentlige sektor skal have muligheden for at benytte cloud computing, hvor det giver værdi og er forsvarligt forretnings- og sikkerhedsmæssigt.*"

EU-Kommissionen ser også gerne, at cloud computing bliver mere udbredt i både den offentlige og private sektor. Det ses f.eks. i Kommissionens strategi fra 2012 for udnyttelse af potentialet ved cloud computing i Europa. Her fremgår det bl.a, at *"Kommissionen tager derfor sigte på at muliggøre og fremme hurtigere indførelse af cloud computing i alle økonomiske sektorer, hvilket kan reducere ikt-omkostningerne og i samspil med nye digitale former for forretningspraksis kan fremme produktiviteten, væksten og beskæftigelsen."*[632]

Nærværende "tema-afsnit" om cloud computing er på den baggrund medtaget i den juridiske analyse af databeskyttelsesforordningen med henblik på at udgøre et *persondataretligt* fundament for det videre arbejde med cloud computing inden for forordningens rammer.

Af Datatilsynets årsberetning fra 2012 fremgår følgende definition af Cloud computing[633]:

"Cloud computing kan defineres som en model for internetbaseret adgang til en delt pulje af konfigurerbare it-ressourcer (net, servere, datalagre, programmer og services), der hurtigt kan etableres og afvikles med en minimal indsats eller interaktion med tjenesteleverandøren. Et eksempel på en cloud-løsning er software udbudt som en service, der ikke skal installeres eller vedligeholdes på kundens egne systemer, men i stedet ligger hos leverandøren og tilgås via brugerens internetbrowser. Som eksempel herpå kan nævnes e-mailtjenester som gmail og hotmail, som er tjenester, der tilgås af brugeren via en inter-

[632] KOM(2012) 529 endelig, s. 2.
[633] Datatilsynets årsberetning 2012, s. 40.

netbrowser, og hvor data ikke gemmes på brugerens egen computer, men i et datacenter hos cloud-leverandøren (i "skyen")."

En tilsvarende definition fremgår af Digitaliseringsstyrelsens arbejdsgrupenotat af 4. juli 2012 om love og regler, der unødigt vanskeliggør anvendelsen af cloud computing. Notatet er offentligt tilgængeligt på styrelsens hjemmeside. Her fremgår bl.a. følgende under overskriften definition af cloud computing og eksempler herpå, s. 3f:

"Ved cloud computing forstås i almindelighed, at visse it-ydelser bliver leveret som en abonnementsordning, således at man som kunde overlader håndteringen af sine data til en leverandør af cloud computing. Kundens adgang til data og applikationer sker ved cloud computing udelukkende via internettet, og kunden har derfor ikke behov for at drive egne servere. Der er således tale om, at en dataansvarlig via internettet og ved brug af distribuerede og forbundne it-systemer lader en databehandler opbevare og behandle oplysninger, herunder personoplysninger.[…]

F.eks. udbydes software i en cloud-løsning som en service, der ikke skal installeres eller vedligeholdes på kundens egne systemer, men i stedet ligger hos leverandøren og tilgås via brugerens internetbrowser. Leverandøren vil placere dataene, hvor dette til enhver tid er mest hensigtsmæssigt for leverandøren. I praksis kan dataene altså – med mindre andet er aftalt – placeres på og flyttes rundt mellem servere i hele verden.

Et eksempel på software leveret som en cloudservice er e-mail-tjenester som gmail og hotmail. Disse tjenester tilgås af brugeren via en internetbrowser. Ved brug af disse tjenester bliver data ikke gemt på brugerens egen computer, men på en server i det, der populært kaldes "skyen" (dvs. i et datacenter hos cloudleverandøren). Der udbydes også andre cloud-produkter som f.eks. regnekraft eller lagerkapacitet over internettet. For alle disse it-ydelser sker der normalt betaling baseret på det faktiske forbrug. […]

Cloud computing adskiller sig fra traditionel outsourcing ved, at ekstern databehandling foregår over internettet, uden at det nødvendigvis er fastlagt på forhånd, hvor data skal eller kan placeres."

5.16.2. Gældende ret

5.16.2.1. Persondataloven mv.

Cloud computing vil typisk indebære en IT-outsourcing til en databehandler, der således udfører en "behandling" i persondatalovens og direktivets forstand i form af *opbevaring* af personoplysninger for den dataansvarlige.

Der kan i forhold til gældende persondataret henvises til Digitaliseringsstyrelsens ovenfor omtalte arbejdsgruppenotat af 4. juli 2012, navnlig notatets afsnit 4, s. 7-18, om gældende ret.

5.16.2.2. Datatilsynets praksis

Datatilsynet har afgivet en række udtalelser om behandlingen af personoplysninger i cloud-løsninger.

Det drejer sig især om tilsynets udtalelse af 3. februar 2011 til Odense Kommune, Datatilsynets j.nr. 2010-52-0138. Sagen drejede sig om kommunens påtænkte brug af Google Apps online kontorpakke med kalender og dokumenthåndtering i forbindelse med kommunens læreres behandling af oplysninger om elever og disses forældre. Der var tale om behandling af bl.a. oplysninger omfattet af persondatalovens §§ 7 og 8, og elever og lærere skulle have adgang til de pågældende oplysninger via personligt brugernavn og en personlig adgangskode.

Datatilsynet udtalte, at tilsynet generelt har en positiv indstilling over for brug af nye teknologier, herunder som udgangspunkt også cloud computing. Samtidig så Datatilsynet det som en af sine væsentlige opgaver at sætte fokus på, at den teknologiske udvikling også kan indebære en øget risiko i forhold til personers ret til privatliv og databeskyttelse. Datatilsynet fastslog, at det niveau for databeskyttelse, som i Danmark er fastlagt ved persondataloven og sikkerhedsbekendtgørelsen, som minimum skal iagttages ved brug af cloud computing. I forhold til de konkrete planer, som Odense Kommune havde, opstod der efter Datatilsynets opfattelse en række spørgsmål i forhold til denne lovgivning.[634]

Datatilsynet pegede på følgende fem forhold, der rejser persondataretlige udfordringer ved brug af cloud computing:

1. Eventuel overførsel af oplysninger til datacentre, som er beliggende i andre usikre tredjelande end USA (at kravet ikke blev stillet i forhold til USA, skyldes at Google Inc.'s datacentre var tilsluttet den dagældende Safe Harbor-ordning), forudsætter, at der er et lovligt grundlag for overførslen, f.eks. at der er indgået en aftale baseret på EU-Kommissionens standardkontrakt, og at der er søgt tilladelse fra Datatilsynet (det sidste er der dog ikke længere krav om efter indsættelsen af § 27, stk. 5, der trådte i kraft 1. januar 2013).

[634] Persondataloven med kommentarer (2015), s. 551f.

2. Den risikovurdering, som Odense Kommune havde foretaget, var efter Datatilsynets opfattelse ikke tilstrækkelig i forhold til kravene i persondatalovens § 41, stk. 3. Datatilsynet anbefalede, at ENISA's tjekliste benyttes.[635]

3. Databehandleraftalen, som påtænktes alene at skulle bestå i elementer fra Googles generelle betingelser, levede ikke op til persondatalovens krav (i § 41, stk. 1, og § 42, stk. 2) om, at Odense Kommune skal sikre, at Google udelukkende må handle efter instruks fra kommunen, ligesom det heller ikke fremgik af databehandleraftalen, at sikkerhedsbekendtgørelsen gælder for databehandlingerne hos Google.

4. Datatilsynet stillede spørgsmål ved, hvordan Odense Kommune kan leve op til persondatalovens krav i § 42, stk. 1, om kontrol med, om sikkerhedsforanstaltningerne overholdes hos databehandleren, når kommunen ikke ved, hvor oplysningerne fysisk befinder sig.

5. Det var uoplyst eller kunne ikke anses for tilstrækkeligt godtgjort ud fra det foreliggende, hvordan sikkerhedsbekendtgørelsens og persondatalovens krav vil blive opfyldt på en række punkter, herunder

a. Sletning af data, så de ikke kan genskabes, jf. sikkerhedsbekendtgørelsens § 9 og persondatalovens § 5, stk. 5.
b. Transmission og login. Det er ikke oplyst, om der sker kryptering mellem Google i Irland og Google Inc.'s forskellige datacentre. Med hensyn til login via internet med adgang til følsomme personoplysninger henstiller Datatilsynet brug af en løsning med flere faktorer, f.eks. digital signatur.
c. Kontrol med afviste adgangsforsøg. Der foreligger ikke oplysninger om automatisk afvisning ved forsøg på at tilgå data uden om Odense Kommunes login-server, jf. sikkerhedsbekendtgørelsens § 18.
d. Med hensyn til logningskravet efter sikkerhedsbekendtgørelsens § 19 foreligger der ikke nærmere oplysninger om, hvilke oplysninger der logges, eller hvor længe loggen opbevares.

Disse forhold førte Datatilsynet til den konklusion, at tilsynet ikke var enig i Odense Kommunes vurdering af, at fortrolige og følsomme oplysninger om elever og forældre kunne behandles i Google Apps. Samtidig anførte Datatilsynet, at det i lyset af sagens principielle karakter og eventuelt vidtrækkende konsekvenser for borgerne i Odense Kommune, var tilsynets opfattelse, at beslutningen om, hvorvidt en løsning af denne karak-

[635] Datatilsynet henviste her til ENISA i publikationen "Cloud computing - Benefits, risks and recommendations for information security", herunder den tjekliste, som findes på s. 71-82 i ENISA's publikation.

ter skulle anvendes på dette område, burde underkastes en vurdering i kommunens politiske organer.

Der kan også henvises til Datatilsynets udtalelse af 3. april 2012, hvor tilsynet udtalte kritik af KL's håndtering af personoplysninger i forbindelse med overførsel af køreprøvesystem til en cloud-løsning, jf. tilsynets j.nr. 2011-631-0136.

I Datatilsynets udtalelse af 6. juni 2012 tog tilsynet herefter stilling til behandling af personoplysninger i Microsofts cloud-løsning Office 365, jf. tilsynets j.nr. 2011-082-0216. I forlængelse heraf udtalte Datatilsynet sig den 10. juli 2012 om de persondataretlige rammer for, at IT-Universitetet, der er en del af den offentlige forvaltning, kunne anvende den pågældende cloud computing-løsning, jf. tilsynets j.nr. 2012-54-0123 og 2012-54-0124.

I udtalelserne fremkom Datatilsynet med bemærkninger om Microsofts ansvar som henholdsvis databehandler og dataansvarlig, ligesom tilsynet også omtalte en række spørgsmål, som danske dataansvarlige vil skulle tage i betragtning ved brug af Office 365. Datatilsynet udtalte sig i den forbindelse om forhold, både kunden og Microsoft skulle være opmærksom på i forbindelse med indgåelse af en tredjelandskontrakt om overførsel til tredjelande, samt databehandleraftale og underdatabehandleraftaler i forbindelse med cloud-løsningen Office 365, herunder Kommissionens standardkoncepter herfor.

Datatilsynet udtalte sig også om virksomheders og myndigheders pligt til som dataansvarlige, der benytter Microsoft som databehandler, at påse, at kravene om sikkerhedsforanstaltninger overholdes hos databehandleren, jf. herved sidste led i persondatalovens § 42, stk. 1.

Datatilsynet anførte i den forbindelse, med henvisning til sikkerhedsvejledningen, at det i den sammenhæng kan være relevant at indhente en årlig revisionserklæring fra en uafhængig tredjepart. Tilsynet anførte også, at den skriftlige aftale parterne imellem kan bl.a. indeholde udarbejdelse af denne revisionserklæring som en betingelse for at lade behandlingen foretage hos databehandleren.

Datatilsynet udtalte herefter følgende om spørgsmålet om dataansvarliges kontrol med behandling af personoplysninger i cloud-løsningen Office 365:

"Datatilsynet har på denne baggrund umiddelbart ingen indvendinger imod en model, hvor danske dataansvarliges kontrol som udgangspunkt sker ved brug af revisionserklæringer fra en uafhængig tredjepart.

Datatilsynet har i den forbindelse noteret sig, at Microsoft har oplyst at ville samarbejde med kunder, hvis særlige behov ikke er blevet imødekommet i forbindelse med den årlige audit, og at kunder i særlige situationer selv vil kunne foretage kontrol."

Der henvises i øvrigt til disse tilsynsudtalelser om Microsoft Office 365, der dog således ses at give mulighed for inden for gældende regler at kunne benytte en cloud computing-løsning, også for en offentlig myndighed.

Der kan endelig henvises til Datatilsynets udtalelse af 15. januar 2014 til en kommune om brug af dansk databehandler og cloudbaseret underdatabehandler i forbindelse med tredjelandsoverførsel, jf. tilsynets 2013-323-0154. Datatilsynet understregede i udtalelsen, at den dataansvarlige myndighed har ansvaret for, at personoplysninger behandles og beskyttes i overensstemmelse med persondataloven og sikkerhedsbekendtgørelsen, uanset hvor data lagres. Hvis der indgår oplysninger omfattet af anmeldelsespligten til Datatilsynet, skal såvel kapitel 1 og 2 som kapitel 3 i sikkerhedsbekendtgørelsen iagttages, herunder logningskravet i bekendtgørelsens § 19.

5.16.2.3. Artikel 29-gruppens udtalelser

Artikel 29-gruppen har i to udtalelser specifikt behandlet cloud computing og forholdet til databeskyttelsesdirektivet (og berørt emnet i andre udtalelser), nemlig i udtalelse 05/2012 af 1. juli 2012 om cloud computing (WP 196) og udtalelse 02/2015 af 22. september 2015 om C-SIG Code of Conduct on Cloud Computing (WP 232), hvortil der i det hele henvises.

Artikel 29-gruppen udtaler, at *"[d]e fleste af disse risici findes inden for to store områder, nemlig manglende **kontrol over personoplysningerne** og utilstrækkelige informationer om selve databehandlingsopgaven (manglende **gennemsigtighed**)"* (fremhævet her), jf. nærmere WP 196, s. 6-7.

Artikel 29-gruppen opstiller, med udgangspunkt i det nugældende retsgrundlag, en tjekliste for, om cloud-kunder og cloud-udbydere har overholdt reglerne om databeskyttelse, jf. nærmere WP 196, s. 22-25.

Artikel 29-gruppens tjekliste indeholder nærmere retningslinjer for følgende forhold:

- Relationen mellem dataansvarlig og databehandler
- En cloud-kundes ansvar som dataansvarlig
- Sikkerhedsforanstaltninger ved underleverancer
- Overholdelse af grundlæggende databeskyttelsesprincipper

- Kontraktlige sikkerhedsforanstaltninger

Artikel 29-gruppen udtaler i den forbindelse i WP 196, s. 23f, bl.a. følgende om den dataansvarliges *kontrol over personoplysningerne*:

"Pligt til samarbejde: Kunden bør sikre, at udbyderen er forpligtet til at samarbejde med hensyn til kundens ret til at føre kontrol med databehandlingsopgaverne, gøre det lettere at udøve de registreredes rettigheder til at have adgang til, korrigere, og slette deres oplysninger, og (hvis aktuelt) underrette cloud-kunden om en eventuel overtrædelse af reglerne om personoplysninger, der vedrører kundens oplysninger. […]

Logning og audit af databehandling: Kunden bør anmode om logning af de databehandlingsopgaver, udbyderen og dennes underleverandører udfører. Kunden bør have beføjelse til at auditere disse databehandlingsopgaver, men audit via en tredjepart valgt af den [data]ansvarlige og certificering kan også være acceptabel, forudsat at der er sikret fuld gennemsigtighed (f.eks. ved at give mulighed for at få en kopi af et certifikat for en tredjepartsaudit eller en kopi af auditrapporten med bekræftelse af certificeringen)."

Videre udtaler artikel 29-gruppen på s. 24f udtrykkeligt følgende om muligheden for at lægge en årlig revisionserklæring fra en uafhængig tredjepart til grund som led i kontrollen:

"Uvildig verificering eller certificering via en velrenommeret tredjepart kan være en troværdig måde for cloud-udbydere, hvorpå de kan vise, at de overholder deres forpligtelser som præciseret i denne udtalelse. En sådan certificering vil som minimum tilkendegive, at en velrenommeret tredjepartsvirksomhed har auditeret eller gennemgået databeskyttelseskontrolforanstaltningerne i forhold til en anerkendt standard, der opfylder kravene i denne udtalelse. I forbindelse med cloud computing bør potentielle kunder undersøge, om cloudtjenesteudbydere kan tilvejebringe en kopi af dette certifikat for tredjepartsaudit eller også en kopi af auditrapporten med bekræftelse på certificeringen, deriblandt overholdelse af kravene i denne udtalelse.

Individuel audit af oplysninger, der "hostes" i et virtualiseret servermiljø, som betjener flere parter, kan måske teknisk set være upraktisk og kan i nogle tilfælde være med til at øge risikoen ved de fysiske og logiske netværkssikkerhedskontrolforanstaltninger, der er iværksat. I så fald kan en relevant tredjepartsaudit valgt af den [data]ansvarlige anses for at være tilfredsstillende i stedet for en individuel [data]ansvarligs ret til at auditere."

Vedrørende *gennemsigtigheden* udtaler Artikel 29-gruppen (s. 12) bl.a., at

"Gennemsigtighed i "skyen" betyder, at det er nødvendigt for cloud-kunden at blive gjort opmærksom på alle de underleverandører, der bidrager til levering af den pågældende cloudtjenesteydelse, samt beliggenheden af alle de datacentre, hvor personoplysningerne måtte blive behandlet.

Artikel 29-gruppen udtaler som baggrund herfor, at *"[k]un da vil han kunne vurdere, hvorvidt personoplysningerne må videresendes til et såkaldt tredjeland uden for Det Europæiske Økonomiske Samarbejdsområde (EØS), hvor der ikke er sikkerhed for et tilstrækkeligt beskyttelsesniveau i den forstand, hvori udtrykket er anvendt i direktiv 95/46/EF."*

5.16.3. Databeskyttelsesforordningen

Kommissionen anførte i forslaget fra 2012 til databeskyttelsesforordning[636] ikke noget om cloud computing. Kommissionen berørte dog cloud computing i sin meddelelse af samme dato om beskyttelse af privatlivets fred i en forbundet verden - en europæisk databeskyttelsesramme til det 21. århundrede, der opsummerede elementerne i databeskyttelsespakken, bestående af databeskyttelsesforordningen og retshåndhævelsesdirektivet.[637] Her udtaler Kommissionen om forslaget til ny databeskyttelsesretlig ramme:

"I nutidens globaliserede verden overføres personoplysninger på tværs af et stigende antal virtuelle og geografiske grænser og opbevares på servere i mange lande. Flere og flere virksomheder tilbyder ***cloud computing-tjenester****, hvorved kunderne får fjernadgang til servere med henblik på at opbevare data "i skyen". Disse faktorer kræver en forbedring af de aktuelle mekanismer til overførsel af data til tredjelande, bl.a. afgørelser om tilstrækkeligheden af beskyttelsesniveauet – dvs. afgørelser om, at databeskyttelsesstandarden er "tilstrækkelig" i tredjelande – og fornødne garantier såsom standardkontraktbestemmelser eller bindende virksomhedsregler, således at der kan sikres et højt databeskyttelsesniveau i international databehandling, og datastrømmen på tværs af grænserne lettes."*[638] (fremhævet her)

Kommissionen udtalte samtidigt bl.a., at *"[f]or at kunne tage globaliseringens udfordringer op skal vi indføre fleksible redskaber og mekanismer – især til virksomheder, der opererer i hele verden – og samtidig garantere en beskyttelse af personoplysninger, der er uden smuthuller. Kommissionen foreslår følgende foranstaltninger:[…] en styrkelse og forenkling af reglerne om international overførsel til lande, der ikke er omfattet af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, vil lette de lovlige datastrømme til tredjelande, især i kraft af en mere strømlinet og omfattende udnyttelse af redskaber som*

[636] Kommissionens forslag af 25. januar 2012, jf. KOM(2012) 11 endelig.
[637] KOM(2012) 9 endelig.
[638] KOM(2012) 9 endelig, s. 11.

bindende virksomhedsregler, så de kan bruges til at dække [databehandlere] og koncerninterne overførsler, hvilket vil give en bedre afspejling af det stigende antal selskaber, der benytter databehandling, ***især cloud computing****".* (fremhævet her)

Peter Blume har også set databeskyttelsesforordningen således, at den er mere møntet på cloud computing end databeskyttelsesdirektivet. Således har han om forordningsforslaget anført, at *"den valgte regulering medfører ikke et egentligt paradigmeskifte, da den dataansvarlige fortsat er den centrale aktør, men der er næppe tvivl om, at den justerede reguleringsmodel er forårsaget af brugen af cloud computing".*[639] Peter Blume henviser i den forbindelse bl.a. til at *[d]atabehandleren* [i forordningsforslaget] *i en række tilfælde er pålagt en selvstændig handlepligt med heraf følgende ansvar. Databehandleren er selvstændiggjort og er blevet synlig i den retlige tekst."*[640]

Senere har Peter Blume tilsvarende anført, at *"[i] forordningen har cloud først og fremmest betydet, at databehandleren har fået sin egen position".*[641]

I den ovenfor omtalte udtalelse 05/2012 af 1. juli 2012 om cloud computing (WP 196) hæfter Artikel 29-gruppen på s. 25 sig ved – i forhold til muligheden for at benytte cloud computing – det positive i artikel 26 om databehandler og artikel 30 om behandlingssikkerhed i forslaget til databeskyttelsesforordning (bestemmelserne blev til hhv. artikel 28 og artikel 32 i den endelige forordning). Artikel 29-gruppen udtaler i den forbindelse følgende:

"Bedre afvejning af ansvaret mellem [data]ansvarlig og [databehandler]: Artikel 29-Gruppen ser positivt på bestemmelserne i artikel 26 i Kommissionens forslag udkast til generel EU-forordning om databeskyttelse), som har til formål at gøre [databehandlere] mere ansvarlige over for [data]ansvarlige ved at være dem behjælpelige med at sikre overholdelse af især sikkerhedsforpligtelserne og de dermed forbundne forpligtelser. I artikel 30 i forslaget foreslås det, at man indfører en retlig forpligtelse for [databehandleren] til at gennemføre passende tekniske og organisatoriske foranstaltninger. Det præciseres i udkastet til forslag, at en [databehandler], der undlader at efterkomme den [data]ansvarliges instrukser, opfylder betingelserne for at være [data]ansvarlig og er underkastet specifikke regler om fælles kontroludøvelse. Artikel 29-Gruppen mener, at det foreliggende forslag går i den rigtige retning med hensyn til at afbøde den manglende balance, der ofte er kendetegnende i cloud computing-miljøet, hvor kunden (navnlig hvis det er en SMV) kan finde det vanskeligt at udøve den fulde kontrol, der er foreskrevet i databeskyttelseslovgivningen, over, hvordan udbyderen leverer de bestilte tjenester."

[639] Peter Blume, Persondataretten i en brydningstid, 2012, s. 129.
[640] Peter Blume, Persondataretten i en brydningstid, 2012, s. 129.
[641] Peter Blume, Den nye persondataret (2016), s. 204.

Selvom det grundlæggende i ansvarsfordelingen mellem den dataansvarlige og databehandleren klart er fastholdt i forordningen, må det konstateres, at en række bestemmelser af relevans for cloud computing ganske rigtigt er blevet skærpet i forordningen, sammenlignet med direktivet, i forhold til cloud-leverandører.

Således er databehandleres rolle og krav til (under)databehandleraftaler udførligt reguleret i artikel 28, hvor det f.eks. af stk. 10, fremgår, at *"[h]vis en databehandler overtræder denne forordning ved at fastlægge formålene med og hjælpemidlerne til behandling, anses databehandleren for at være en dataansvarlig for så vidt angår den pågældende behandling, uden at dette berører artikel 82, 83 og 84."*

Der henvises i øvrigt til afsnittet ovenfor om artikel 28, ligesom der i den forbindelse kan henvises til det anførte ovenfor om artikel 32 om behandlingssikkerhed, der også forpligter databehandleren direkte og til det anførte nedenfor om artikel 37, hvor det udtrykkeligt af ordlyden i stk. 1 fremgår, at også databehandlere skal udnævne databeskyttelsesrådgivere.

Der kan – i denne cloud-sammenhæng – også henvises til, at reglerne om overførsler til tredjelande også, som en nyskabelse, gør databehandlere til pligtsubjekter, jf. f.eks. artikel 46, stk. 1, ligesom databehandleres erstatnings- og strafansvar også er udtrykkeligt reguleret i artikel 82-83.

5.16.4. Overvejelser

Som nævnt ovenfor udtalte Datatilsynet i sagen om cloud computing i Odense Kommune, at tilsynet generelt har en positiv indstilling over for brug af nye teknologier, såsom cloud computing.

Der er da heller ikke noget i det nuværende databeskyttelsesdirektiv, der forhindrer brugen af cloud computing. Så længe det sker inden for rammerne af direktivets forskellige krav, kan det lade sig gøre persondataretligt.

Databeskyttelsesforordningen forstærker mulighederne for at benytte cloud computing. Selvom cloud computing også i fremtiden givetvis vil være et af de områder inden for persondataretten, der rejser mange spørgsmål, understøtter forordningen en videre udbredelse af cloud computing i såvel den private som offentlige sektor.

Der er således ingen tvivl om, at databeskyttelsesforordningen giver mulighed for, at såvel offentlige som private aktører benytter sig af cloud computing og dermed opnår de effektivitets- og økonomiske fordele, der er forbundet med denne teknologi.

Cloud computing skal naturligvis anvendes inden for rammerne af forordningen (og anden lovgivning), f.eks. kravene heri til databehandleraftaler, til behandlingssikkerheden, til tredjelandsoverførsler og til konsekvensanalyser.

Samtidig ligger det fast, at både den dataansvarlige og databehandlerne har ansvar for overholdelse af forordningen ved benyttelse af cloud computing. Det er dog fortsat den dataansvarlige, der har ansvaret for, at vedkommende alene benytter cloud-leverandører eller databehandlere, der håndterer personoplysninger i overensstemmelse med forordningen, jf. f.eks. forordningens artikel 5, stk. 2, artikel 28, stk. 1, artikel 29 og artikel 32, stk. 4.

5.17. Privates forpligtelse til at udpege en databeskyttelsesrådgiver, artikel 37

5.17.1. Præsentation

Der følger ikke en forpligtelse om at udpege en databeskyttelsesrådgiver efter gældende ret.

Databeskyttelsesforordningen lægger – i modsætning hertil – op til en ordning i artikel 37, hvor bl.a. private dataansvarlige og databehandlere i en række nærmere angivne tilfælde er forpligtede til at udpege en databeskyttelsesrådgiver.

5.17.2. Gældende ret

Der følger som nævnt ikke en forpligtelse om at udpege en databeskyttelsesrådgiver efter gældende ret. Det følger imidlertid af databeskyttelsesdirektivets artikel 18, stk. 2, 2. pind, at medlemsstaterne har mulighed for enten at indføre en forenkling af anmeldelsespligten eller fritage helt fra denne forpligtelse, hvilket bl.a. forudsætter indførelsen af en ordning med en databeskyttelsesrådgiver.

Da direktivet skulle implementeres i dansk ret, var det således muligt at indføre en ordning med udpegelse af en databeskyttelsesrådgiver.

Det følger dog af Registerudvalgets betænkning nr. 1345, at der ikke på daværende tidspunkt fandtes en konstruktion i dansk ret svarende til scenariet med en databeskyttelsesrådgiver i direktivets artikel 18, stk. 2, 2. pind.[642] På baggrund af overvejelser af arbejdsretlig og ledelsesmæssig karakter og hensynet til at erhvervslivet ikke pålægges unødige byr-

[642] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 336.

der, endte Registerudvalget med at anbefale, at der ikke indførtes en sådan ordning med en databeskyttelsesrådgiver i dansk ret i stedet for en generel anmeldelsesordning.[643]

5.17.3. Databeskyttelsesforordningen

Det følger af forordningens artikel 37, stk. 1, at den dataansvarlige og databehandleren altid udpeger en databeskyttelsesrådgiver, når denne er omfattet af ét af de tre tilfælde, der opregnes i artikel 37, stk. 1, litra a-c.

Det første tilfælde, hvor en dataansvarlig eller databehandler altid skal udpege en databeskyttelsesrådgiver følger af artikel 37, stk. 1, litra a. Dette tilfælde omfatter alene behandling af oplysninger, der foretages af en offentlig myndighed eller et offentligt organ, undtagen domstole, der handler i deres egenskab af domstol. For en nærmere gennemgang heraf henvises til afsnit 5.18. om offentlige myndigheders udpegelse af en databeskyttelsesrådgiver.

Det følger derudover af artikel 37, stk. 1, litra b, at den dataansvarlige eller databehandleren altid skal udpege en databeskyttelsesrådgiver, når dennes kerneaktiviteter består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål kræver regelmæssig og systematisk overvågning af registrerede i stort omfang.

Endelig følger det af artikel 37, stk. 1, litra c, at den dataansvarliges eller databehandlerens altid skal udpege en databeskyttelsesrådgiver, når dennes kerneaktiviteter består af behandling i stort omfang af særlige kategorier af oplysninger, jf. artikel 9, og personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10.

Artikel 37, stk. 1, litra b og litra c, vedrører alene private dataansvarlige og databehandlere, jf. forordningens præambelbetragtning nr. 97.

5.17.3.1. Kerneaktivitetsbegrebet i artikel 37, stk. 1, litra b og litra c

Fælles for de to tilfælde i henholdsvis artikel 37, stk. 1, litra b og litra c, er for det første, at der henvises til den dataansvarlige og databehandlerens *kerneaktiviteter*.

Det følger således af de to bestemmelser, at der skal være tale om *kerneaktiviteter*, førend den dataansvarlige eller databehandleren er omfattet af forpligtelsen til altid at skulle udpege en databeskyttelsesrådgiver efter forordningens artikel 37, stk. 1.

[643] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 337.

Forståelsen af begrebet "kerneaktiviteter" i artikel 37, stk. 1, litra b og litra c, suppleres af præambelbetragtning nr. 97, hvorefter den dataansvarliges og databehandlerens kerneaktivitet i den private sektor vedrører vedkommendes hovedaktiviteter og ikke behandling af personoplysninger som biaktivitet.

Det må betyde, at selvom en organisation eller en virksomhed regelmæssigt behandler personoplysninger som en del af deres foretagende, medfører dette ikke nødvendigvis, at behandlingen er omfattet af begrebet *kerneaktiviteter* efter artikel 37, stk. 1. litra b og litra c.

Det må således antages, at dataansvarlige og databehandlere der alene behandler oplysninger om personoplysninger som en biaktivitet i forbindelse med f.eks. kundekontakt- og support, salg, personaleadministration mv., ikke er omfattet af begrebet kerneaktiviteter efter forordningen.

Omvendt må det antages, at dataansvarlige og databehandlere, der tilbyder et produkt, der *består* i behandling af personoplysninger, må anses for at have behandling af personoplysninger som en hovedaktivitet og dermed være omfattet af begrebet kerneaktiviteter. Som eksempler herpå kan nævnes organisationer eller virksomheder, der tilbyder hosting eller lagring af personoplysninger, herunder cloud-løsninger og udbydere af marketingsundersøgelser.

Det kan ligeledes antages, at behandlingsaktiviteter foretaget af den dataansvarlige og databehandlere, der tilbyder et produkt, der er *uløseligt* forbundet med behandlingen af personoplysninger, også anses for kerneaktiviteter efter artikel 37, stk. 1, litra b og litra c. Dette er tilfældet, hvis det pågældende produkt er baseret på behandling af personoplysninger i så høj grad, at der er tale om en kerneaktivitet.

Et eksempel kunne være privathospitaler, der som produkt udbyder patientbehandling. En sådan behandling vil i så høj grad basere sig på hospitalets behandling af personoplysninger, herunder især følsomme oplysninger om helbredsmæssige forhold efter forordningens artikel 9, at dette må anses for omfattet af begrebet kerneaktivitet.[644]

Et andet eksempel herpå er forsikringsselskaber, der udbyder forsikringer på baggrund af personoplysninger indsamlet om kommende og nuværende kunder. I et sådant tilfælde vil produktet (forsikringsydelsen) også være uløseligt forbundet med behandlingen af personoplysninger således, at der også her er tale om kerneaktiviteter efter forordningens artikel 37, stk. 1, litra b og litra c.

[644] Artikel 29-gruppens udtalelse nr. 16/2016 om 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01), pkt. 2.1.2.

Omvendt må det antages, at f.eks. skoler og døgninstitutioner – i det omfang disse ikke er omfattet af artikel 37, stk. 1, litra a, om offentlige myndigheder og organer – ikke behandler personoplysninger på en sådan måde, der er uløseligt forbundet med selve undervisningsydelsen eller pasningsydelsen, selvom institutionerne behandler oplysninger om børn og deres forældre i et vist omfang.

Dette må eksempelvis også antages normalt at gøre sig gældende for forsyningsselskaber, idet disse ikke kan anses for at behandle personoplysninger som kerneaktivitet på en sådan måde, der er uløseligt forbundet med selve det at sælge og distribuere f.eks. fjernvarme og vandforsyning, selvom forsyningsselskaber i den forbindelse naturligvis behandler kundeoplysninger i et vist omfang. Noget andet ville være tilfældet, hvis det pågældende forsyningsselskab begynder at udbyde et produkt, der består i at videresælge personoplysninger.

5.17.3.2. Begrebet "i et stort omfang" i artikel 37, stk. 1, litra b og litra c

Dernæst er det fælles for artikel 37, stk. 1, litra b og litra c, at der også skal være tale om en behandling, der foretages *i et stort omfang*, før der skal udpeges en databeskyttelsesrådgiver.

Det er ikke i forordningen defineret, hvad der skal betegnes som "i et stort omfang". I præambelbetragtning nr. 91, der dog omhandler konsekvensanalyse, kan der formentlig indhentes et fortolkningsbidrag hertil, idet der beskrives, hvornår der efter forordningen er tale om "omfattende behandlingsaktiviteter".

Det følger af præambelbetragtningen, at omfattende behandlingsaktiviteter indebærer behandling af meget store mængder af personoplysninger på regionalt, nationalt eller overnationalt plan, der kan berøre mange registrerede personer, og som sandsynligvis vil indebære en høj risiko.

Endvidere følger det af betragtningen, at behandling af personoplysninger ikke bør anses for at være omfattende, hvis der er tale om en læges, sundhedspersonales eller en advokats behandling af personoplysninger om patienter eller klienter.

Der angives således to yderpunkter til, hvad der efter forordningen kan anses for "omfattende behandlingsaktiviteter".

Herudover må det antages, at der med ordlyden "i et stort omfang" i artikel 37, stk. 1, litra b og litra c, både kan henvises til mængden af oplysninger, der behandles, men også til antallet af registrerede personer, der behandles oplysninger om.

Artikel 29-gruppen anbefaler i deres udtalelse om databeskyttelsesrådgivere, at der ved vurderingen af, om der er tale om behandling af personoplysninger "i et stort omfang", lægges vægt på fire kriterier.[645] For det første bør der – ifølge Artikel 29-gruppen – lægges vægt på antallet af personer, der behandles oplysninger om, enten det specifikke antal personer eller som andele af den relevante population. Dernæst bør der lægges vægt på volumen af personoplysninger og rækkevidden af de forskellige personoplysninger, der bliver behandlet. Endvidere bør der lægges vægt på tidsperioden, som der behandles oplysninger i, samt hvorvidt behandlingen er permanent. Endelig bør den geografiske udstrækning af behandlingsaktiviteterne indgå.

På baggrund af ovenstående vil en behandling af f.eks. patientdata på et hospital anses for behandling i et stort omfang efter forordningens artikel 37, stk. 1, litra b og litra c.[646] Dette vil formentlig endvidere være tilfældet for behandlingen af kundeoplysninger i forsikringsselskaber eller banker.[647]

En behandling af oplysninger for virksomheder, der udøver adfærdsbaseret annoncering, udbyder en søgemaskine eller er en telefoni- og/eller internetudbyder, må ligeledes anses for behandling i et stort omfang.[648]

På den anden side kan behandling af patientdata i en lægepraksis med et begrænset antal læger tilknyttet formentlig ikke anses for behandling af oplysninger i et stort omfang. Det samme må formentlig gøre sig gældende for behandlingen af klientoplysninger i et mindre advokatfirma. Det bemærkes, at f.eks. et advokatfirma kun vil være omfattet af kravet om at skulle udpege en databeskyttelsesrådgiver, hvis de øvrige betingelser, herunder kravet om kerneaktivitet, er opfyldt. (Sidstnævnte må normalt ikke antages at være tilfældet i forbindelse med advokatvirksomhed.)

5.17.3.3. Regelmæssig og systematisk overvågning af de registrerede – særligt vedrørende artikel 37, stk. 1, litra b

Udover de to fælles betingelser for artikel 37, stk. 1, litra b og litra c, skal de specifikt opregnede tilfælde i bestemmelserne være til stede, såfremt forpligtelsen om at udpege en databeskyttelsesrådgiver indtræder.

[645] Artikel 29-gruppens udtalelse nr. 16/2016 om 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01), pkt. 2.1.3.
[646] Artikel 29-gruppens udtalelse nr. 16/2016 om 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01), pkt. 2.1.3.
[647] Artikel 29-gruppens udtalelse nr. 16/2016 om 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01), pkt. 2.1.3.
[648] Artikel 29-gruppens udtalelse nr. 16/2016 om 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01), pkt. 2.1.3.

For så vidt angår artikel 37, stk. 1, *litra b*, skal der også være tale om en kerneaktivitet, der består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål *kræver regelmæssig og systematisk overvågning af registrerede* i et stort omfang.

I præambelbetragtning nr. 24 kan der findes et fortolkningsbidrag til, hvad der skal forstås ved "overvågning af registreredes adfærd", der i øvrigt ikke er nærmere defineret i forordningen. Det følger således af præambelbetragtningen, at for at afgøre, om en behandlingsaktivitet kan betragtes som overvågning af registreredes adfærd, bør det undersøges, om fysiske personer spores på internettet, herunder mulig efterfølgende brug af teknikker til behandling af personoplysninger, der består i profilering af en fysisk person, navnlig med det formål at træffe beslutninger om den pågældende eller analysere eller forudsige den pågældendes præferencer, adfærd og holdninger.

Selvom præambelbetragtningen omhandler forordningens territoriale anvendelsesområde, må den antages at kunne yde et vist fortolkningsbidrag for så vidt angår, hvad der skal forstås ved "regelmæssig og systematisk overvågning" efter forordningens artikel 37, stk. 1, litra b.

Det betyder, at regelmæssig og systematisk overvågning af de registrerede i hvert fald omfatter alle former for sporing (tracking) og profilering via internettet.

Dog kan det bemærkes, at der i præambelbetragtning nr. 24 alene er fokus på overvågning via internettet. Der er ikke holdepunkter i ordlyden af artikel 37, stk. 1, litra b, for at antage, at *regelmæssig og systematisk overvågning af de registrerede* ikke også kan omfatte overvågning, der ikke sker via internettet.[649]

Det fremgår af Artikel 29-gruppens udtalelse om databeskyttelsesrådgivere, at "regelmæssig og systematisk overvågning af de registrerede" f.eks. må antages at omfatte drift af telekommunikationsnetværk eller services forbundet hermed, profilering i forbindelse med risikovurdering, herunder kreditvurdering, lokalitetstracking via applikationer samt adfærdsbaseret annoncering mv.[650]

5.17.3.4. Særlige kategorier af oplysninger – særligt vedrørende artikel 37, stk. 1, litra c
Det følger specifikt af artikel 37, stk. 1, *litra c*, at der – når de to fællesbetingelser i artikel 37, stk. 1, litra a og b er opfyldt – også skal udpeges en databeskyttelsesrådgiver, når den

[649] Artikel 29-gruppens udtalelse nr. 16/2016 om 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01), pkt. 2.1.4.
[650] Artikel 29-gruppens udtalelse nr. 16/2016 om 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01), pkt. 2.1.4.

dataansvarliges eller databehandlerens kerneaktiviteter består af behandling i stort omfang af *særlige kategorier af oplysninger*, jf. artikel 9, og personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10.

Det betyder, at såfremt en behandlingsaktivitet omfatter følsomme oplysninger som opregnet i artikel 9, stk. 1, eller oplysninger om straffedomme og lovovertrædelser i artikel 10, stk. 1, og denne udgør *kerneaktiviteter* og sker i *et stort omfang*, skal den dataansvarlige eller databehandleren altid udpege en databeskyttelsesrådgiver. Det forhold, at der behandles følsomme oplysninger såsom oplysninger om fagforeningsmæssigt tilhørsforhold eller oplysninger om helbredsmæssige forhold i forbindelse med f.eks. en virksomheds personaleadministration medfører ikke i sig selv et krav om, at der skal udpeges en databeskyttelsesrådgiver. Hertil kræves nemlig, at de øvrige krav om *kerneaktivitet* og behandling *i et stort omfang* af følsomme oplysninger omfattet af artikel 9 eller af artikel 10 er opfyldt.

Følsomme oplysninger efter forordningens artikel 9, stk. 1, er oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

5.17.3.5. Udnævnelse af fælles databeskyttelsesrådgiver

Forordningens artikel 37, stk. 2, giver mulighed for, at en koncern kan udnævne en fælles databeskyttelsesrådgiver forudsat, at alle etableringer har let adgang til databeskyttelsesrådgiveren.

En koncern er defineret i forordningens artikel 4, nr. 19, som en virksomhed, der udøver kontrol, og de af denne kontrollerede virksomheder.

Det må antages, at artikel 37, stk. 2, har til formål at tilgodese koncerner, som agerer i flere medlemsstater på én gang.

Det fremgår af artikel 37, stk. 2, at der ikke nævnes øvrige muligheder for andre private end koncerner til at udpege en fælles databeskyttelsesrådgiver.

Det må imidlertid antages, at forordningens artikel 37, stk. 2, er udtryk for, hvornår en privat dataansvarlig eller en databehandler *kan* udpege en fælles databeskyttelsesrådgiver. Der er således ikke holdepunkter for at antage, at artikel 37, stk. 2, skal forstås som en udtømmende opregning af, i hvilke tilfælde private kan udpege en fælles databeskyttelsesrådgiver.

Det betyder, at andre private dataansvarlige og databehandlere end koncerner også har mulighed for at udpege en fælles databeskyttelsesrådgiver, hvilket også følger af det forhold, at det må antages, at et konsulentfirma kan udøve funktionen som databeskyttelsesrådgiver for flere dataansvarlige på samme tid på baggrund af tjenesteydelseskontrakter.

Det er dog en forudsætning for, at private kan udpege en fælles databeskyttelsesrådgiver, at denne kan efterleve forordningens krav til stilling, opgaver, uafhængighed samt tilgængelighed efter artikel 37 til 39, når opgaven løses for flere private dataansvarlige og/eller databehandlere på én gang.

Det skal ligeledes bemærkes, at forordningens krav til en databeskyttelsesrådgiver om bl.a. tilgængelighed og uafhængighed alt andet lige må antages at forudsætte nogle særlige overvejelser i forhold til efterlevelse, når denne udøver sin funktion for flere dataansvarlige og/eller databehandlere på én gang.

Det er således forordningens krav til en databeskyttelsesrådgivers funktion, stilling og opgaver i artikel 37-39, der begrænser privates mulighed for at udpege en fælles databeskyttelsesrådgiver, herunder kravene om tilgængelighed, interessekonflikt samt tilstrækkelig opgavehåndtering.

5.17.3.6. Offentliggørelse af den databeskyttelsesansvarliges kontaktoplysninger, artikel 37, stk. 7

Det følger af forordningens artikel 37, stk. 7, at den dataansvarlige eller databehandleren offentliggør kontaktoplysninger for databeskyttelsesrådgiveren og meddeler disse til tilsynsmyndigheden.

Formålet med kravet om offentliggørelse er, at såvel de registrerede som tilsynsmyndigheder let skal kunne komme i kontakt med den pågældende dataansvarliges eller databehandlers databeskyttelsesrådgiver.

5.17.4. Overvejelser

Med forordningens artikel 37 sker der en ændring i forhold til gældende ret, idet der nu fastsættes en forpligtelse for bl.a. private dataansvarlige og databehandlere til i visse tilfælde altid at skulle udpege en databeskyttelsesrådgiver.

Der skal dog meget til, før private dataansvarlige *skal* udpege end databeskyttelsesrådgiver. Følgende betingelser, der er gennemgået ovenfor, *skal* således alle være opfyldt for, at private virksomheder skal udpege en databeskyttelsesrådgiver: Behandlingen af personoplysninger skal for det *første* være virksomhedens kerneaktivitet. For det andet *skal* der be-

handles personoplysninger i et stort omfang. Endelig skal behandlingsaktiviteten for det *tredje* bestå i regelmæssig og systematisk overvågning af personer *eller* behandlingen skal vedrøre følsomme oplysninger i stort omfang (artikel 9- og 10-oplysninger).

Der er endvidere en mulighed for, at en flerhed af private dataansvarlige og/eller databehandlere udpeger en fælles databeskyttelsesrådgiver, så længe databeskyttelsesrådgiveren kan efterleve forordningens krav i artikel 37-39, når rollen udføres for flere private på én gang.

5.18. Offentlige myndigheder og organers forpligtelse til at udpege en databeskyttelsesrådgiver, artikel 37

5.18.1. Præsentation

Der følger ikke en forpligtelse om at udpege en databeskyttelsesrådgiver efter gældende ret.

Databeskyttelsesforordningen lægger – i modsætning hertil – op til en ordning i artikel 37, hvor bl.a. offentlige dataansvarlige og databehandlere altid i en række nærmere angivne tilfælde er forpligtede til at udpege en databeskyttelsesrådgiver.

5.18.2. Gældende ret

Der henvises til afsnit 3.17. om privates udpegning af en databeskyttelsesrådgiver.

5.18.3. Databeskyttelsesforordningen

5.18.3.1. Offentlig myndighed eller offentligt organ

Det følger af artikel 37, stk. 1, *litra a*, at den dataansvarlige og databehandleren altid udpeger en databeskyttelsesrådgiver, når behandlingen foretages af en offentlig myndighed eller et offentligt organ, undtagen domstole, der handler i deres egenskab af domstole.

Det er ikke nærmere i forordningen defineret, hvad der udgør en "offentlig myndighed" eller et "offentligt organ".

Det følger bl.a. af præambelbetragtning nr. 45, sidste punktum, at det bør henhøre under EU-retten eller medlemsstaternes nationale ret at afgøre, om den dataansvarlige, der udfører en opgave i samfundets interesse eller i forbindelse med offentlig myndighedsudøvelse, skal være en offentlig myndighed eller en anden fysisk eller juridisk person, der er omfattet af offentlig ret, eller, hvis dette er i samfundets interesse, af privatret som f.eks. en erhvervssammenslutning.

Medlemsstaterne må herefter selv afgøre, om behandling af oplysninger i forbindelse med udførelse af opgaver i samfundets interesse eller offentlig myndighedsudøvelse skal håndteres af offentlige myndigheder, offentlige organer (i præambelbetragtningen benævnt som bl.a. en juridisk person, der er omfattet af offentlig ret) eller private.

Det må betyde, at medlemsstaterne selv afgør, hvilke enheder, der er omfattet af begreberne "en offentlig myndighed" og "et offentligt organ" og dermed omfattet af medlemsstaternes offentlige ret.[651]

På den baggrund, og da begreberne "en offentlig myndighed" og "et offentligt organ" i øvrigt ikke er defineret i forordningen, må det antages, at begreberne udfyldes af medlemsstaterne i overensstemmelse med deres traditionelle afgrænsning af det offentlige.

I en dansk kontekst vil de myndigheder, der i dansk ret henregnes til den offentlige forvaltning, jf. forvaltningslovens § 1, stk. 1-2, således være omfattet af artikel 37, stk. 1, litra a, og kravet om at udpege en databeskyttelsesrådgiver.

Af forvaltningslovens § 1, stk. 1-2, fremgår, at følgende virksomhed omfattes af loven: al virksomhed, der udøves af den offentlige forvaltning, og al virksomhed, der udøves af selvejende institutioner, foreninger, fonde mv., der er oprettet ved lov eller i henhold til lov, eller er oprettet på privatretligt grundlag og udøver offentlig virksomhed af mere omfattende karakter og er undergivet intensiv offentlig regulering, intensivt offentligt tilsyn og intensiv offentlig kontrol.

For så vidt angår selvejende institutioner mv. oprettet på privatretligt grundlag (forvaltningslovens § 1, stk. 2, nr. 2), vil der således være nogle, som omfattes af kravet om at have en databeskyttelsesrådgiver, mens andre ikke omfattes af kravet.

I det omfang man ved *særlovgivning* har reguleret, at forvaltningsloven finder anvendelse for private organisationer, vil der ikke være tale om en offentlig myndighed i forordningens forstand.

For en nærmere gennemgang af afgræsningen af den offentlige forvaltning i forvaltningsloven henvises til Niels Fenger, Kommentarer til forvaltningsloven, 1. udgave (2013), s. 64-75.

[651] Artikel 29-gruppens udtalelse nr. 16/2017 om Guidelines on Data Protection Officers (WP 243 rev.01), pkt. 2.1.1.

5.18.3.2. Fælles databeskyttelsesrådgiver

Det følger af artikel 37, stk. 3, at hvis den dataansvarlige eller databehandleren er en offentlig myndighed eller et offentligt organ, kan en fælles databeskyttelsesrådgiver udpeges for flere af sådanne myndigheder eller organer i overensstemmelse med *deres organisatoriske struktur og størrelse*.

Det er en forudsætning for, at der kan udpeges en fælles databeskyttelsesrådgiver, at denne kan efterleve forordningens krav til en databeskyttelsesrådgiver, herunder til dennes stilling, opgaver, uafhængighed samt tilgængelighed efter forordningens artikel 37 til 39, når opgaven løses for flere dataansvarlige eller databehandlere på én gang.[652] Det skal ligeledes bemærkes, at forordningens krav til en databeskyttelsesrådgiver om bl.a. tilgængelig og uafhængighed alt andet lige må antages at forudsætte nogle særlige overvejelser i forhold til efterlevelse, når denne udøver sin funktion for flere dataansvarlige eller databehandlere.

Der kan på baggrund af ordlyden i artikel 37, stk. 3, skitseres forskellige situationer, hvor offentlige myndigheder og/eller organer henholdsvis kan og ikke kan udpege en fælles databeskyttelsesrådgiver.

En kommune er et eksempel på en offentlig myndighed, som i nogen tilfælde vil kunne dele en databeskyttelsesrådgiver. Det springende punkt er, om man som databeskyttelsesrådgiver for f.eks. en større kommune, kan efterleve sin funktion retmæssigt, når funktionen også udøves for andre kommuner.

Det kan på baggrund af ordlyden i artikel 37, stk. 3, antages, at det *ikke* er "i overensstemmelse med en offentlig myndigheds struktur og størrelse", hvis en fælles databeskyttelsesrådgiver fungerer på baggrund af én ansættelseskontrakt i f.eks. to forskellige kommuner.

I modsætning hertil må det dog antages, at det er i overensstemmelse med bestemmelsens ordlyd, at en databeskyttelsesrådgiver udøver sin funktion på baggrund af to deltidskontrakter i to kommuner på samme tid. Den retlige grænse for at dele en databeskyttelsesrådgiver vil i et sådant tilfælde være de gældende standarder om offentligt ansattes bierhverv og de almindelige habilitetsregler.[653]

Dette må ligeledes antages at gøre sig gældende, når en databeskyttelsesrådgiver har ansættelse i én kommune og er ansat på baggrund af en tjenesteydelseskontrakt i en anden kommune.

[652] Artikel 29-gruppens udtalelse nr. 16/2016 om 'Guidelines on Data Protection Officers ('DPOs')', (WP 243 rev.01), s. 10.
[653] F.eks. vejledning om "god adfærd i det offentlige".

Det må endvidere antages, at to eller flere kommuner kan oprette et kommunalt fællesskab, jf. § 60 i lov om kommunernes styrelse[654], til hvilket de kan gå sammen om at løse opgaven som databeskyttelsesrådgiver i de deltagende kommuner.

Endelig må det antages, at et konsulentfirma kan udøve funktionen som databeskyttelsesrådgiver for flere offentlige myndigheder og/eller organer på samme tid på baggrund af tjenesteydelseskontrakter.

Det vil dog være et krav, at der er én, der er personligt ansvarlig for hvervet som databeskyttelsesrådgiver for hver myndighed.

For så vidt angår kommuner, hvor det på baggrund af ovenstående ikke er muligt at dele en databeskyttelsesrådgiver, skal det bemærkes, at den pågældende kommune ikke vil skulle udpege en databeskyttelsesrådgiver for de enkelte forvaltninger mv., men vil kunne udpege én databeskyttelsesrådgiver for hver kommune. Dette skyldes, at en kommune normalt må anses for at være dataansvarlig for alle de behandlinger af personoplysninger, som foretages inden for den kommunale enhedsforvaltning.

Som yderligere eksempler på myndigheder, som *kan* udpege en fælles databeskyttelsesrådgiver, kan nævnes politiet. Det vil således ikke være nødvendigt for hver enkelt politikreds at udpege en databeskyttelsesrådgiver. Det samme gør sig gældende for f.eks. ministerier, hvor departement og underordnede myndigheder ikke nødvendigvis skal udpege hver sin databeskyttelsesrådgiver. Omvendt må politiet anses for at være så stor en enhed, at politiet ikke kan dele databeskyttelsesrådgiver med andre myndigheder under Justitsministeriets ressort.

Herudover kan det nævnes, at forskellige myndigheder og/eller organer, der formentlig kan dele en databeskyttelsesrådgiver, er styrelser, der er organiseret således, at de udøver en sekretariatsfunktion for et eller flere uafhængige nævn. Dette må formentlig ligeledes gøre sig gældende for kommuner, der sekretariatsbetjener beboerklagenævn samt Børne- og Ungeudvalg.

Endelig kan det bemærkes, at myndigheder, som også vil kunne dele en databeskyttelsesrådgiver, er selvejende institutioner, som gennemfører undervisningsaktiviteter inden for ensartede rammer, der følger af lovgivningen om de enkelte institutionstyper, f.eks. uddannelsesinstitutioner undergivet den samme lovgivning – også selv om den enkelte institution i sit virke som selvejende institution skal være uafhængig og have sin egen bestyrelse. Det

[654] Bekendtgørelse af lov om kommunernes styrelse, lovbekendtgørelse nr. 318 af 28. marts 2017.

betyder, at f.eks. en gruppe af institutioner for almengymnasiale uddannelser – eller andre uddannelsesinstitutioner omfattet af samme lovgivning – kan vælge at have en fælles databeskyttelsesrådgiver.

5.18.4. Overvejelser

Med forordningens artikel 37 sker der en ændring i forhold til gældende ret, idet der nu fastsættes en forpligtelse for dataansvarlige og databehandlere, der er offentlige myndigheder og organer til altid at skulle udpege en databeskyttelsesrådgiver.

Dog er det muligt for flere offentlige myndigheder og organer at udpege en fælles databeskyttelsesrådgiver, så længe databeskyttelsesrådgiveren kan efterleve forordningens krav til stilling, opgaver, uafhængighed samt tilgængelighed efter forordningens artikel 37 til 39.

5.19. Artikel 37, stk. 4, bl.a. om muligheden for danske særregler

Det følger af artikel 37, stk. 4, at der i andre tilfælde end de i stk. 1 omhandlede *kan* eller, når det kræves i henhold til EU-retten eller medlemsstaternes nationale ret, *skal* den dataansvarlige eller databehandleren eller sammenslutninger og andre organer, som repræsenterer kategorier af dataansvarlige eller databehandlere, udpege en databeskyttelsesrådgiver. Databeskyttelsesrådgiveren kan handle på vegne af sådanne sammenslutninger og andre organer, som repræsenterer dataansvarlige eller databehandlere.

Det betyder, at den dataansvarlige og databehandleren i visse tilfælde alligevel skal udpege en databeskyttelsesrådgiver, hvis det kræves i henhold til EU-retten eller national ret.

Endvidere kan den dataansvarlige og databehandleren frivilligt vælge at udpege en databeskyttelsesrådgiver på baggrund af artikel 37, stk. 4.

I de tilfælde, hvor der frivilligt udpeges en databeskyttelsesrådgiver, må de samme krav gælde til databeskyttelsesrådgiverens stilling, kvalifikationer og opgaver mv. efter forordningens artikel 37-39, som hvis den dataansvarlige eller databehandleren var forpligtet til at udpege en databeskyttelsesrådgiver.[655]

[655] Artikel 29-gruppens udtalelse nr. 16/2016 om 'Guidelines on Data Protection Officers ('DPOs')', (WP 243 rev.01), pkt. 2.1.

5.20. Databeskyttelsesrådgiverens stilling og kvalifikationer, artikel 37, stk. 5-6, og artikel 38

5.20.1. Præsentation

I databeskyttelsesforordningens artikel 37, stk. 5-6, og artikel 38 er der krav til databeskyttelsesrådgiverens stilling.

Artikel 37, stk. 5-6, vedrører krav en databeskyttelsesrådgivers kvalifikationer og regler om den tilknytning, som rådgiveren kan have til den dataansvarlige eller databehandleren.

Artikel 38 vedrører krav til inddragelse af databeskyttelsesrådgiveren, krav til støtte af rådgiveren med ressourcer og rådgiverens adgang til oplysninger og behandlingsaktiviteter, regler om beskyttelse af stillingen som databeskyttelsesrådgiver, krav om, at rådgiveren skal være et kontaktpunkt for den registrerede, regler om databeskyttelsesrådgiverens tavshedspligt og fortrolighed samt regler om, at rådgiveren kan udføre andre opgaver og have andre forpligtelser.

5.20.2. Gældende ret

Der henvises til afsnit 3.17. om privates forpligtelse til at udpege en databeskyttelsesrådgiver.

5.20.3. Databeskyttelsesforordningen

5.20.3.1. Indledning

Ifølge Kommissionens begrundelse for forslaget til forordningen[656] bygger kravet om en databeskyttelsesrådgiver på databeskyttelsesdirektivets artikel 18, stk. 2, som gav medlemsstaterne mulighed for at indføre et sådant krav i stedet for en generel anmeldelsespligt.

Den endelige ordlyd af forordningens bestemmelser om databeskyttelsesrådgiver svarer med visse ændringer til artikel 35-37 i Kommissionens forslag.

Formålet med ordningen med en databeskyttelsesrådgiver er at understøtte den dataansvarliges og databehandlerens sikring af overholdelsen af forordningen og dermed at understøtte forordningens røde tråd om ansvarlighed ("accountability"), som afspejles i artikel 24, stk. 1, om den dataansvarliges ansvar.

[656] Punkt 3.4.4.4 i begrundelsen til Kommissionens forslag, KOM(2012) 11 endelig, af 27. januar 2012 til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

5.20.3.2. Faglige kvalifikationer

I de tilfælde, hvor dataansvarlige og databehandlere skal udpege en databeskyttelsesrådgiver, jf. artikel 37, stk. 1 og 4, er den dataansvarlige og databehandleren efter artikel 37, stk. 5, forpligtede til at udpege databeskyttelsesrådgiveren på grundlag af dennes faglige kvalifikationer, navnlig ekspertise inden for databeskyttelsesret samt evne til at udføre de opgaver, der er omhandlet i artikel 39.

I lyset af formålet med ordningen med en databeskyttelsesrådgiver og opgaverne opregnet i artikel 39 må det anses for en forudsætning, at den dataansvarlige eller databehandleren udpeger en person med uddannelse og erfaring, der gør, at denne person er i stand til at vurdere om konkrete påtænkte eller igangværende behandlingsaktiviteter overholder forordningens regler og andre relevante databeskyttelsesretlige regler.

Det følger af præambelbetragtning nr. 97, 2. sidste pkt., at den nødvendige ekspertise navnlig bør fastsættes i henhold til de databehandlingsaktiviteter, der foretages, og den beskyttelse de personoplysninger, som den dataansvarlige eller databehandleren behandler, kræver.

Den nærmere fastlæggelse af, hvad der skal forstås ved udtrykket '*ekspertise inden for databeskyttelsesret og -praksis*', må endvidere skulle ses i lyset af databeskyttelsesrådgiverens opgaver, der er opregnet i artikel 39. På baggrund heraf må der ved udtrykket antages at sigte mod en person med juridiske kompetencer inden for databeskyttelsesret, som har en vis erfaring med at håndtere sådanne spørgsmål. Niveauet vil afhænge af mængden, følsomheden og kompleksiteten af de oplysninger, der behandles.

Det kan dog ikke med forordningen antages at være et krav, at man som databeskyttelsesrådgiver skal have en bestemt uddannelsesmæssig baggrund, såsom f.eks. jurist.

Hvis der udpeges en databeskyttelsesrådgiver fra den dataansvarliges eller databehandlerens egen organisation, kan det med fordel være en person, som i forvejen har et vist kendskab eller indsigt med håndtering af databeskyttelsesretlige spørgsmål i organisationen.

Herudover bør databeskyttelsesrådgiveren som følge af, at det i almindelighed må kunne kræves, at databeskyttelsesrådgiveren har evne til at udføre de omhandlede opgaver, have et kendskab til forordningens bestemmelser og andre relevante databeskyttelsesretlige regler.

5.20.3.3. Kontraktmæssig tilknytning til den dataansvarlige eller databehandleren
Efter artikel 37, stk. 6, kan databeskyttelsesrådgiveren være den dataansvarliges eller databehandlerens medarbejder, eller rådgiveren kan udføre hvervet på grundlag af en tjenesteydelseskontrakt.

Herved åbnes mulighed for, at hvervet som databeskyttelsesrådgiver kan besættes ved at udpege en medarbejder, der allerede er ansat, eller ved besættelse af en stilling hos den dataansvarlige eller databehandleren, eller ved at den dataansvarlige eller databehandleren får opgaven udført med ekstern bistand ved en tjenesteydelseskontrakt, f.eks. med et advokatfirma eller et revisionsfirma. I hvilket omfang en ekstern rådgiver kan fungere som databeskyttelsesrådgiver for flere dataansvarlige og databehandlere må nærmere afgøres af habilitetsregler, der gælder for den pågældende branche, såsom de advokatetiske regler eller de gældende standarder om offentligt ansattes bierhverv og de almindelige habilitetsregler[657] mv.

5.20.3.4. Inddragelse af databeskyttelsesrådgiveren
Ifølge forordningens artikel 38, stk. 1, skal den dataansvarlige og databehandleren sikre, at databeskyttelsesrådgiveren inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger.

5.20.3.4.1. Spørgsmål vedrørende beskyttelse af personoplysninger
Det skal således sikres, at databeskyttelsesrådgiveren inddrages i "alle spørgsmål vedrørende beskyttelse af personoplysninger".

Idet forordningen må anses for at være en nærmere udmøntning af retten til beskyttelse af personoplysninger[658], må kravet om inddragelse forstås bredt, således at det som udgangspunkt omfatter alle spørgsmål om den dataansvarliges og databehandlerens overholdelse af de regler i forordningen, som den dataansvarlige eller databehandleren skal overholde. Henset til, at databeskyttelsesrådgiverens opgaver i henhold til artikel 39, stk. 1, litra a og b, også omfatter EU-ret eller national ret i medlemsstaterne om databeskyttelse, indebærer dette, at databeskyttelsesrådgiveren også skal inddrages i spørgsmål om overholdelsen af sådanne regler.

Dette indebærer således, at databeskyttelsesrådgiveren skal inddrages i alle de overvejelser og vurderinger, som det forudsættes, at den dataansvarlige eller databehandleren har gjort

[657] F.eks. vejledning om "god adfærd i det offentlige".
[658] Artikel 8, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 16, stk. 1, i traktaten om Den Europæiske Unions Funktionsmåde.

sig og foretaget med henblik på at overholde forordningens regler og andre relevante EU-retlige og nationale regler om databeskyttelse.

Det vil sige, at databeskyttelsesrådgiveren skal inddrages ved vurderingen af, om de behandlinger af personoplysninger, som foretages eller iværksættes for den dataansvarlige eller databehandleren, overholder reglerne i forordningens kapitel II om de grundlæggende behandlingsprincipper og behandlingsbetingelserne.

Det vil f.eks. være overvejelser og vurderinger af, om behandlingen på baggrund af det udtrykkeligt angivne formål er saglig, proportional eller kræver samtykke fra den registrerede.

I forhold til reglerne om den registreredes rettigheder vil databeskyttelsesrådgiveren endvidere skulle inddrages i overvejelser om, hvorvidt og hvorledes de registreredes rettigheder skal efterleves, herunder i forbindelse med at den dataansvarlige skal træffe passende foranstaltninger for efterlevelsen, jf. forordningens artikel 12, eller databehandlerens bistand med efterlevelsen ved hjælp af passende foranstaltninger, jf. artikel 28.

Yderligere vil databeskyttelsesrådgiveren skulle inddrages i forbindelse med den dataansvarliges og databehandlerens overvejelser om overholdelsen af deres forpligtelser efter forordningens kapitel IV, herunder fastsættelse af sikkerhedsforanstaltninger, jf. artikel 32, samt passende foranstaltninger, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, og passende foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun nødvendige personoplysninger behandles, jf. artikel 25.

Desuden er det i relation til konsekvensanalyser vedrørende databeskyttelse efter artikel 35 præciseret i bestemmelsens stk. 2, at den dataansvarlige skal rådføre sig med databeskyttelsesrådgiveren, hvis en sådan er udpeget, når der foretages en konsekvensanalyse vedrørende databeskyttelse. Her er det således nærmere angivet, hvilken karakter inddragelsen af rådgiveren skal have.

5.20.3.4.2. Sikring af inddragelse
Ifølge artikel 38, stk. 1, skal inddragelsen som nævnt ovenfor sikres af den dataansvarlige og databehandleren.

I lyset af at det efter artikel 38, stk. 3, skal sikres, at databeskyttelsesrådgiveren ikke modtager instruktion, må den dataansvarlige og databehandleren i medfør af stk. 1 anses for at være forpligtede til at holde databeskyttelsesrådgiveren tilstrækkeligt og rettidigt orienteret om alle spørgsmål om beskyttelse af personoplysninger samt mulighed for at vurdere over-

holdelsen af forordningens og andre relevante databeskyttelsesretlige regler og komme med bemærkninger eller lignende.

Den dataansvarlige eller databehandleren kan således ikke bestemme, at databeskyttelsesrådgiveren skal involvere sig. Dog kan databeskyttelsesrådgiveren være forpligtet efter reglerne i artikel 39 til at bistå med rådgivning, hvor der må være behov herfor.

5.20.3.4.3. Tilstrækkelig og rettidig inddragelse
Som nævnt ovenfor følger det af bestemmelsen, at inddragelsen af databeskyttelsesrådgiveren skal være *tilstrækkelig* og *rettidig*.

Dette spørgsmål skal ses i sammenhæng med databeskyttelsesrådgiverens formål, opgaver og princippet om ansvarlighed, som er udtrykt i artikel 24.

På baggrund heraf må det anses at være et krav, at databeskyttelsesrådgiveren inddrages i så god tid, som det er muligt og relevant, forud for iværksættelse af behandlingsaktiviteter i et sådant omfang, at rådgiveren er i stand til at vurdere, om de påtænkte behandlingsaktiviteter overholder forordningens regler og komme med kvalificerede bemærkninger herom inden iværksættelsen, med henblik på at yde den dataansvarlige eller databehandleren rådgivning i overensstemmelse med artikel 39, stk. 1, litra a. Det samme må anses at gøre sig gældende i forhold til ændringer i igangværende behandlingsaktiviteter, men også i forbindelse med overvejelser og udstedelse af retningslinjer, procedurer mv. for, hvorledes forordningen og andre relevante databeskyttelsesretlige regler skal overholdes.

Således vil databeskyttelsesrådgiveren eksempelvis skulle inddrages forud for beslutningen om, hvilke foranstaltninger der efter artikel 25 er passende med henblik på databeskyttelse gennem design og standardindstillinger.

Det vil forekomme, at kravet om, at der udpeges en databeskyttelsesrådgiver, indtræder efter behandlingsaktiviteter er iværksat. I den forbindelse må databeskyttelsesrådgiveren umiddelbart efter udpegelsen inddrages i tilstrækkeligt omfang til at kunne vurdere, om de igangværende behandlingsaktiviteter overholder forordningens regler, bl.a. med henblik på at yde rådgivning i overensstemmelse med artikel 39, stk. 1, litra a, og med henblik på at overvåge overholdelsen af forordningen i overensstemmelse med artikel 39, stk. 1, litra b.

Endelig må kravet om, at inddragelsen skal være tilstrækkelig, antages at indebære at den dataansvarlige eller databehandleren i sine overvejelser og fastlæggelse af de interne foranstaltninger med henblik på overholdelsen af forordningen skal inddrage og tage højde for

databeskyttelsesrådgiverens bemærkninger og rådgivning i øvrigt samt dennes rapportering om overholdelsen af forordningen og andre databeskyttelsesregler.

5.20.3.5. Ressourcer og adgang
Efter artikel 38, stk. 2, skal den dataansvarlige og databehandleren støtte databeskyttelsesrådgiveren i forbindelse med udførelsen af de i artikel 39 omhandlede opgaver ved at tilvejebringe de ressourcer, der er nødvendige for at udføre disse opgaver og opretholde databeskyttelsesrådgiverens ekspertise, samt adgang til personoplysninger og behandlingsaktiviteter.

Bestemmelsen indebærer, at den dataansvarlige og databehandleren skal stille de fornødne faciliteter og arbejdsredskaber, økonomiske ressourcer, personaleressourcer og lignende til rådighed for databeskyttelsesrådgiveren. Denne vurdering er den dataansvarlige eller databehandleren ansvarlig for.

Bestemmelsen må også antages at indebære, at den ansatte databeskyttelsesrådgiver skal have tid nok til opgaverne. Har databeskyttelsesrådgiveren også andre opgaver og forpligtelser i overensstemmelse med artikel 38, stk. 6, må disse andre opgaver således ikke gå ud over den tid, det kræver at udføre opgaverne som databeskyttelsesrådgiver.

Som nævnt i ovenstående afsnit skal databeskyttelsesrådgiveren inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger i et omfang, så rådgiveren er i stand til at vurdere, om behandlingsaktiviteterne overholder forordningens regler samt relevante EU-retlige og nationale regler om databeskyttelse, ligesom databeskyttelsesrådgiveren skal inddrages i den fortløbende kontrol med og sikring af reglernes overholdes, herunder i forbindelse med udarbejdelse af databeskyttelsespolitikker eller lignende retningslinjer til sikring af overholdelse af reglerne.

Den nærmere fastlæggelse af, hvor mange ressourcer der kræves til støtte for databeskyttelsesrådgiveren, afhænger af de organisatoriske forhold hos den dataansvarlige og databehandleren, herunder størrelsen af den dataansvarliges eller databehandlerens organisation, antallet af behandlingsaktiviteter, omfanget af de enkelte behandlingsaktiviteter, herunder antallet af registrerede og kategorierne af oplysninger, samt kompleksiteten af og de forbundne risici med disse behandlingsaktiviteter.

Det må generelt kunne forventes, at behovet for ressourcer til støtte for databeskyttelsesrådgiveren vil være større i en stor organisation med mange omfattende behandlingsaktiviteter med høj kompleksitet og store forbundne risici end i en lille organisation med få behandlingsaktiviteter af lav kompleksitet med mindre risici.

Endelig indebærer bestemmelsen som nævnt ovenfor, at databeskyttelsesrådgiveren skal støttes ved at tilvejebringe adgang til personoplysninger og behandlingsaktiviteter.

Adgangen er ikke nærmere angivet i bestemmelsen, men det må generelt antages, at der skal være tale om en vid adgang, som kan tilvejebringes efter behov. Kravet hænger bl.a. sammen med databeskyttelsesrådgiverens overvågningsopgave efter artikel 39, stk. 1, litra b.

5.20.3.6. Uafhængighed og beskyttelse af stilling

Efter artikel 38, stk. 3, skal den dataansvarlige og databehandleren sikre, at databeskyttelsesrådgiveren ikke modtager instrukser vedrørende udførelsen af disse opgaver, ligesom den pågældende ikke må afskediges eller straffes af den dataansvarlige eller databehandleren for at udføre sine opgaver. Endvidere følger det af bestemmelsen, at databeskyttelsesrådgiveren rapporterer direkte til det øverste ledelsesniveau hos den dataansvarlige eller databehandleren.

Det fremgår af forordningens præambelbetragtning nr. 97, sidste punktum, at databeskyttelsesrådgivere, uanset om de er ansat hos den dataansvarlige eller ej, bør være i stand til at udøve deres hverv på uafhængig vis.

5.20.3.6.1. Uafhængighed

Artikel 38, stk. 3, 1. pkt., indebærer, at databeskyttelsesrådgiveren ikke må blive instrueret af andre om, hvordan rådgiveren skal udføre de opgaver, der er opregnet i forordningens artikel 39.[659]

Rammerne for hvordan databeskyttelsesrådgiveren skal udføre opgaverne som databeskyttelsesrådgiver, skal således findes i forordningens artikel 39. Der henvises til afsnit 5.21. om databeskyttelsesrådgiverens opgaver, artikel 39 og artikel 35, stk. 2.

I kravet om, at databeskyttelsesrådgiveren ikke må blive instrueret, må det anses for forudsat, at databeskyttelsesrådgiveren ved udførelsen af opgaverne i artikel 39 ikke er underlagt nogen ledelse hos den dataansvarlige eller databehandleren, men alene forordningens anvisninger.

Kravet om uafhængighed betyder, at databeskyttelsesrådgiveren f.eks. *ikke* må instrueres i, hvorvidt der skal foretages høring af tilsynsmyndigheden mv. Databeskyttelsesrådgiveren

[659] Henvisningen med udtrykket '*disse opgaver'* til de opgaver i artikel 39, der er omtalt i den forudgående bestemmelse i stk. 2.

må heller ikke direkte eller indirekte få besked på at komme til et "bestemt resultat", når vedkommende opererer som databeskyttelsesrådgiver.

Rådgiveren kan imidlertid være underlagt instruktion og ledelse ved udførelsen af andre opgaver og forpligtelser, jf. artikel 38, stk. 6, så længe disse opgaver og pligter ikke medfører en interessekonflikt. Se nærmere herom nedenfor under afsnit 5.20.3.9.

I tilknytning hertil indebærer bestemmelsens *3. pkt.*, at databeskyttelsesrådgiveren alene *rapporterer* til den øverste ledelse. Der er således heller ikke herved indlagt muligheder for påvirkning af rådgiverens udførelse af sine opgaver, men derimod synes det at være tilsigtet, at databeskyttelsesrådgiveren uvildigt skal bistå den dataansvarliges eller databehandlerens øverste ledelse med overholdelsen af forordningens regler og andre EU-retlige og nationale databeskyttelsesregler. Ifølge artikel 39 skal dette bl.a. ske ved at overvåge overholdelsen og rådgive om forpligtelserne.

Der fremgår ikke nærmere fortolkningsbidrag af forordningen om, hvad der skal forstås ved *den øverste ledelse*.

I lyset af databeskyttelsesrådgiverens ovennævnte rapporterende og rådgivende funktion må det imidlertid antages, at det herved tilsigtes, at databeskyttelsesrådgiveren rapporterer direkte dertil, hvor det overordnede ansvar for den daglige drift reelt ligger, og hvor de overordnede beslutningerne herfor træffes.

Hvor i den dataansvarliges eller databehandlerens organisation, dette ledelsesniveau er, afhænger af organiseringen hos den konkrete dataansvarlige eller databehandleren.

I myndigheder, der ledes af én politiker, må den øverste ledelse forstås som den øverste administrative ledelse.

For så vidt angår kommuner og regioner, må der lægges vægt på, at disse er administrative myndigheder, hvis øverste ledelse er et politisk valgt kollegialt organ. På den baggrund på forordningen forstås sådan, at databeskyttelsesrådgiveren skal rapportere direkte til kommunalbestyrelsen henholdsvis regionsrådet, og at denne rapportering forelægges for kommunalbestyrelsen henholdsvis regionsrådet uden den forudgående udvalgsbehandling, som de kommunale og regionale sager ellers normalt skal undergives.

Forordningen regulerer ikke den organisatoriske placering af databeskyttelsesrådgiveren hos den dataansvarlige eller databehandleren. For kommuner og regioners vedkommende betyder det, at databeskyttelsesrådgiveren vil indgå som en almindelig del af forvaltningen

og være underlagt et udvalg. Økonomi- og Indenrigsministeriet vil efter en konkret vurdering efter § 65 c i lov om kommuners styrelse henholdsvis regionslovens § 36 meddele dispensation til, at databeskyttelsesrådgiveren organiseres direkte under kommunalbestyrelsen henholdsvis regionsrådet.

I forhold til det private erhvervsliv kan det bemærkes, at i selskabsloven er det bestyrelsen, der er det centrale eller øverste ledelsesorgan i selskaber, der både har en bestyrelse og en direktion. Når der i databeskyttelsesforordningen henvises til det øverste ledelsesniveau, må det i det private forstås i relation til den daglige drift og dermed direktionen, såfremt selskabet har både en bestyrelse og en direktion. Det vil i praksis betyde, at direktionen skal orientere bestyrelsen om væsentlige forhold, som påpeges af databeskyttelsesrådgiveren.

5.20.3.6.2. Beskyttelse af stilling

Bestemmelsens *2. pkt.* indebærer, at databeskyttelsesrådgiveren er beskyttet mod afskedigelse eller sanktioner for at udføre sine opgaver i henhold til artikel 39. Beskyttelsen af stillingen er med til at sikre den tilsigtede uafhængighed og uvildighed.

Normalt kan man i Danmark ikke afskediges for at udføre sine arbejdsopgaver, og beskyttelsen i artikel 38, stk. 3, 2. pkt., peger således i retning af en almindelig saglighedsbeskyttelse, som den kommer til udtryk i funktionærloven.

Omvendt er der ikke noget til hinder for, at databeskyttelsesrådgiveren afskediges på et sagligt grundlag, f.eks. hvis vedkommende ikke udfører sine opgaver efter artikel 39 eller i øvrigt misligholder ansættelsesforholdet væsentligt ved f.eks. at stjæle fra arbejdspladsen. Databeskyttelsesrådgiveren vil kunne afskediges på et *sagligt* grundlag efter almindelige arbejdsretlige regler. Overtrædelse af beskyttelsen i artikel 38, stk. 3, 2. pkt., kan medføre bødestraf efter forordningens artikel 83, stk. 4, litra a.

5.20.3.7. Kontaktpunkt for den registrerede

Den registrerede kan efter artikel 38, stk. 4, kontakte databeskyttelsesrådgiveren angående alle spørgsmål om behandling af deres oplysninger og om udøvelse af deres rettigheder i henhold til denne forordning.

Bestemmelsen må i tråd med det grundlæggende princip om gennemsigtighed, som bl.a. er udtrykt i forordningens artikel 5, stk. 1, litra a[660], anses for at indebære, at databeskyttelses-

[660] Gennemsigtighed er endvidere omtalt i præambelbetragtning nr. 39, 78 og 100, ligesom udtrykket er anvendt i titlen til forordningens kapitel 3, afdeling 1, samt artikel 88, stk. 2, om behandling i forbindelse med ansættelsesforhold.

rådgiveren ved kontakt med den registrerede – hvis der er anledning hertil – skal vejlede den registrerede om behandlingsaktiviteter, som omfatter oplysninger om den pågældende.

Databeskyttelsesrådgiveren skal endvidere vejlede om, hvilke rettigheder den registrerede har, og hvordan de kan udnyttes. Dette er endvidere i tråd med den dataansvarliges forpligtelse efter artikel 12, stk. 2, om at lette udøvelsen af den registreredes rettigheder.

Kontakten med de registrerede og vejledningen må anses for at understøtte databeskyttelsesrådgiverens opgaver, herunder i særdeleshed opfyldelse af formålet om kontrol og herved opgaven med at overvåge overholdelsen af de databeskyttelsesretlige regler i forordningen, EU-ret og national ret, jf. artikel 39, stk. 1, litra b. Herved kan databeskyttelsesrådgiveren bl.a. blive gjort opmærksom på behandlinger, der ikke overholder reglerne, eller procedurer, der ikke fungerer efter hensigten.

Bestemmelsen hænger sammen med kravet i artikel 37, stk. 7, til den dataansvarlige eller databehandleren, om at kontaktoplysninger for databeskyttelsesrådgiveren skal offentliggøres. Endvidere vil de registrerede som led i oplysningspligten efter forordningens artikel 13 og 14 som udgangspunkt modtage kontaktoplysninger for databeskyttelsesrådgiveren sammen med en række andre oplysninger om den behandlingsaktivitet, som omfatter behandling af oplysninger om den pågældende registrerede. Kontaktoplysninger for databeskyttelsesrådgiveren vil også blive oplyst ved underretning til den registrerede om brud på persondatasikkerheden sammen med en række andre oplysninger om bl.a. sikkerhedsbruddet.

5.20.3.8. Tavshedspligt og fortrolighed

Derudover følger det af artikel 38, stk. 5, at databeskyttelsesrådgiveren er underlagt tavshedspligt eller fortrolighed vedrørende udførelsen af sine opgaver i overensstemmelse med EU-retten eller medlemsstaternes nationale ret.

Bestemmelsen må på baggrund af ordvalget antages at overlade det til EU-retten eller medlemsstaternes nationale lovgivning, om databeskyttelsesrådgiveren i det konkrete tilfælde skal være underlagt tavshedspligt eller fortrolighed. I en dansk kontekst vil det f.eks. være forvaltningslovens § 27 og straffelovens § 152-152 f, der medfører tavshedspligt eller fortrolighed.

5.20.3.9. Andre forenelige opgaver og pligter

Endelig følger det af artikel 38, stk. 6, at databeskyttelsesrådgiveren kan udføre andre opgaver og have andre pligter. Dog skal den dataansvarlige eller databehandleren efter bestemmelsen sikre, at sådanne opgaver og pligter ikke medfører en interessekonflikt.

På baggrund af kravet om uafhængighed og under hensyn til uvildigheden af den rådgivning, som databeskyttelsesrådgiveren bistår med, må dette betyde, at databeskyttelsesrådgiveren ikke samtidig med dette hverv kan være *ansvarlig* for den dataansvarliges eller databehandlerens behandlingsaktiviteter, herunder for persondataretlige regler – f.eks. sikkerhedskravene – overholdes i organisationen.

Dermed kan en databeskyttelsesrådgiver formentlig normalt ikke være den øverste IT-ansvarlige eller øverste HR-ansvarlige i en organisation. Derimod kan medarbejdere, som ikke har det øverste ansvar herfor, have hvervet som databeskyttelsesrådgiver.

I lyset af formålet med databeskyttelsesrådgiverordningen, dennes opgaver og at det af artikel 38, stk. 1, fremgår, at databeskyttelsesrådgiveren "inddrages tilstrækkeligt og rettidigt i alle spørgsmål om beskyttelse af personoplysninger" kan vedkommende dog nødvendigvis ikke være afskåret fra at være en aktiv del af overvejelserne og beslutningerne om, hvordan det sikres i organisationen, at de databeskyttelsesretlige regler overholdes. En sådan rolle ses allerede i flere virksomheder som en "compliance officer".

Databeskyttelsesrådgiveren må således kunne inddrages i organisationens implementering af de krav, der følger af forordningen. Dermed skal databeskyttelsesrådgiveren f.eks. inddrages i forbindelse med indkøb af nyt IT-system og dertilhørende overvejelser om databeskyttelse gennem design og gennem standardindstillinger efter artikel 25, herunder i forbindelse med formulering af kravspecifikationer til leverandører.

Databeskyttelsesrådgiveren kan og skal også involveres i f.eks. udarbejdelsen af organisationens politikker på databeskyttelsesområdet.

5.20.4. Overvejelser

Med forordningens artikel 37-38, er der tale om en nyskabelse i forhold til gældende ret, idet der fremover stilles krav om udpegelse af en databeskyttelsesrådgiver i visse tilfælde, og at denne skal have en bestemt uafhængig stilling og bestemte kvalifikationer.

Kravene til databeskyttelsesrådgiverens stilling og kvalifikationer er forholdsvis detaljeret reguleret i forordningen.

Forpligtelsen til at udpege en databeskyttelsesrådgiver ændrer dog ikke i sig selv på de databeskyttelsesretlige krav, som vedkommende skal rådgive organisationen om. Som det i øvrigt fremgår af denne betænkning, er kravene i databeskyttelsesforordningen således i vidt omfang en videreførelse af kravene i databeskyttelsesdirektivet og dermed persondataloven.

5.21. Databeskyttelsesrådgiverens opgaver, artikel 39 og 35, stk. 2

5.21.1 Præsentation
Forordningens artikel 39 indeholder en beskrivelse af databeskyttelsesrådgiverens opgaver.

5.21.2 Gældende ret
Der henvises til afsnit 5.17. om privates forpligtelse til at udpege en databeskyttelsesrådgiver, artikel 37.

5.21.3 Databeskyttelsesforordningen
I medfør af forordningens artikel 39, stk. 1, påhviler en række opgaver databeskyttelsesrådgiveren. I artiklen reguleres det, hvilke opgaver der *som minimum* påhviler databeskyttelsesrådgiveren.

Der er ikke noget til hinder for, at den dataansvarlige overlader flere opgaver til databeskyttelsesrådgiveren, end de opgaver, som fremgår af forordningens artikel 39, eller at databeskyttelsesrådgiverens opgaver beskrives nærmere, f.eks. i en (ansættelses)aftale med databeskyttelsesrådgiveren.

Det fremgår af forordningens artikel 39, stk. 1, at databeskyttelsesrådgiveren som minimum har følgende opgaver:

a) at *underrette og rådgive* den dataansvarlige eller databehandleren og de ansatte, der behandler personoplysninger, om deres forpligtelser i henhold til databeskyttelsesforordningen og anden EU-ret eller national ret i medlemsstaterne om databeskyttelse
b) at *overvåge* overholdelsen af databeskyttelsesforordningen, af anden EU-ret eller national ret i medlemsstaterne om databeskyttelse og af den dataansvarliges eller databehandlerens politikker om beskyttelse af personoplysninger, herunder fordeling af ansvar, oplysningskampagner og uddannelse af personale, der medvirker ved behandlingsaktiviteter, og de tilhørende revisioner
c) at *rådgive*, når der anmodes herom, med hensyn til *konsekvensanalysen* vedrørende databeskyttelse og overvåge dens opfyldelse i henhold til artikel 35
d) at *samarbejde* med tilsynsmyndigheden
e) at fungere som tilsynsmyndighedens *kontaktpunkt* i spørgsmål vedrørende behandling, herunder den forudgående høring, der er omhandlet i artikel 36, og at høre tilsynsmyndigheden, når det er hensigtsmæssigt, om eventuelle andre spørgsmål.

Det vil være hensigtsmæssigt, hvis den dataansvarlige i øvrigt klart definerer, hvilke opgaver som påhviler databeskyttelsesrådgiveren, herunder i forbindelse med konsekvensanalysen.

5.21.3.1 Underrette og rådgive
Databeskyttelsesrådgiveren skal i medfør af artikel 39, stk. 1, litra a, underrette og rådgive den dataansvarlige eller databehandleren og de ansatte, der behandler personoplysninger, om deres forpligtelser i henhold til forordningen og anden EU-ret eller national ret i medlemsstaterne om databeskyttelse.

Bestemmelsen skal ses i sammenhæng med artikel 38, stk. 1, hvorefter den dataansvarlige og databehandleren sikrer, at databeskyttelsesrådgiveren inddrages tilstrækkeligt og rettidigt i *alle* spørgsmål vedrørende beskyttelse af personoplysninger. Det er således klart, at databeskyttelsesrådgiveren generelt skal kunne rådgive om beskyttelse af personoplysninger, også på områder, hvor eventuelle forpligtelser ikke følger af databeskyttelsesforordningen.

I relation til forpligtelserne i henhold til forordningen vil et vigtigt element i databeskyttelsesrådgiverens opgave være rådgivning om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, således som det nærmere er beskrevet i artikel 25. Også i forbindelse med førelse af fortegnelser over behandlingsaktiviteter efter artikel 30 vil databeskyttelsesrådgiveren have en væsentlig opgave i relation til rådgivning om overholdelse af forordningen.

Databeskyttelsesrådgiverens opgave består også i at stå til rådighed, således at f.eks. ansatte har mulighed for at henvende sig til databeskyttelsesrådgiveren og anmode om rådgivning mv.

5.21.3.2 Overvåge overholdelsen af databeskyttelsesforordningen
Centralt for databeskyttelsesrådgiveren er den i artikel 39, stk. 1, litra b, anførte opgave med at overvåge overholdelsen af databeskyttelsesforordningen. Som led i denne opgave kan databeskyttelsesrådgiveren f.eks. foretage følgende:

- indsamle oplysninger til at identificere behandlingsaktiviteter
- analysere og kontrollere lovlighed af behandlingsaktiviteter
- informere, rådgive og komme med anbefalinger til den dataansvarlige og databehandleren.

Det bemærkes i den forbindelse, at det følger af artikel 24, at det er den dataansvarlige, som er ansvarlig for at gennemføre passende tekniske og organisatoriske foranstaltninger

for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med forordning. Databeskyttelsesrådgiverens opgave med at overvåge overholdelsen af forordningen medfører ikke, at databeskyttelsesrådgiveren overtager dette ansvar. Ansvaret påhviler den dataansvarlige eller databehandleren.

5.21.3.3 Databeskyttelsesrådgiverens rolle i konsekvensanalysen
Som det fremgår af artikel 39, stk. 1, litra c, skal databeskyttelsesrådgiveren rådgive med hensyn til konsekvensanalysen, når der anmodes herom.

Det følger på tilsvarende vis af forordningens artikel 35, stk. 2, at den dataansvarlige rådfører sig med databeskyttelsesrådgiveren (hvis en sådan er udpeget), når der foretages en konsekvensanalyse vedrørende databeskyttelse.

I den forbindelse kan den dataansvarlige f.eks. anmode databeskyttelsesrådgiveren om rådgivning vedrørende følgende:

- om der skal gennemføres en konsekvensanalyse
- hvilken fremgangsmåde der skal anvendes ved gennemførelse af konsekvensanalysen
- om konsekvensanalysen kan gennemføres internt, eller om gennemførelsen kræver antagelse af ekstern bistand
- hvilke sikkerhedsforanstaltninger (tekniske og organisatoriske) som skal anvendes for at begrænse risici i forhold til de registreredes rettigheder og interesser
- om konsekvensanalysen er korrekt gennemført og om dens konklusioner er i overensstemmelse med forordningen.

I tilfælde af uenighed mellem den dataansvarlige eller databehandleren og databeskyttelsesrådgiveren kan det specifikt fremgå af konsekvensanalysen, hvorfor databeskyttelsesrådgiverens indstilling ikke er blevet fulgt. Dette er dog ikke et krav til konsekvensanalysen.

5.21.3.4 Samarbejde med tilsynsmyndigheden mv.
Det følger af artikel 39, stk. 1, litra d og e, at databeskyttelsesrådgiveren skal samarbejde med tilsynsmyndigheden og fungere som tilsynsmyndighedens kontaktperson vedrørende behandling, herunder den forudgående høring, der er omhandlet i artikel 36, og at høre tilsynsmyndigheden, når det er hensigtsmæssigt, om eventuelle andre spørgsmål.

Litra d og e er på sin vis en nærmere udmøntning af artikel 31 i tilfælde, hvor der er udpeget en databeskyttelsesrådgiver. Efter bestemmelsen i artikel 31 samarbejder den dataan-

svarlige og databehandleren samt, hvis det er relevant, deres repræsentanter efter anmodning med tilsynsmyndigheden i forbindelsen med udførelsen af dens opgaver.

5.21.3.5 Risikohensyn
Det følger af artikel 39, stk. 2, at databeskyttelsesrådgiveren under udførelsen af sine opgaver tager behørigt hensyn til den risiko, der er forbundet med behandlingsaktiviteter, under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål.

Databeskyttelsesrådgiveren skal således prioritere sine opgaver og fokusere på de behandlingsaktiviteter, som konkret indebærer højere grader af risiko, uden at overvågning af overholdelse af forordningen på områder, som indebærer en lavere grad af risiko, helt undlades.

5.21.4 Overvejelser
Det er ikke i alle tilfælde, at der skal udpeges en databeskyttelsesrådgiver. I de tilfælde, hvor en databeskyttelsesrådgiver skal udpeges får vedkommende efter artikel 38 og 39 en central rådgivningsrolle i organisationen. Denne rolle kan med fordel udmøntes nærmere i en (ansættelses)kontrakt.

5.22. Adfærdskodekser, artikel 40

5.22.1. Præsentation
Efter persondatalovens § 74 kan brancheforeninger eller andre organer, som repræsenterer andre kategorier af private dataansvarlige, i samarbejde med Datatilsynet udarbejde adfærdskodekser, der skal bidrage til en korrekt anvendelse af reglerne i loven. Persondatalovens § 74 har sin baggrund i artikel 27 i databeskyttelsesdirektivet.

Bestemmelsen i persondatalovens § 74 ses indtil videre ikke at have haft nogen praktisk betydning i Danmark. Dette synes også i et vist omfang at være tendensen i de øvrige EU-medlemsstater. I hvert fald har Kommissionen i en meddelelse om en global metode til beskyttelse af personoplysninger i EU fra 2010[661], forud for sit forslag til databeskyttelsesforordning fra 2012[662], bl.a. udtalt, at de gældende bestemmelser om selvregulering i databeskyttelsesdirektivet, nemlig muligheden for udarbejdelse af adfærdskodekser, hidtil sjældent er blevet anvendt, og at private interessenter ikke finder dem tilfredsstillende.

[661] KOM(2010) 609 endelig af 4. november 2010, s. 13.
[662] Kommissionens forslag af 25. januar (KOM (2012) 11 endelig), s. 11.

Ovennævnte udtalelse fra Kommissionen har således formentlig været medvirkende til, at der i databeskyttelsesforordningens artikel 40 om adfærdskodekser opstilles mere specifikke krav til adfærdskodeksers udfærdigelse, indhold og anvendelse. Det er stadig frivilligt, om man vil følge en godkendt adfærdskodeks eller ej, men overholdelsen af godkendte kodekser kan nu anvendes som et element til at påvise overholdelse af den dataansvarliges forpligtelser i henhold til forordningen, jf. artikel 24, stk. 3, og samtidig kan det lette arbejdet med den praktiske implementering af forordningen, og eventuelt medvirke til at reducere en bødes størrelse.

5.22.2. Gældende ret

5.22.2.1. Persondatalovens § 74

Af persondatalovens § 74 fremgår det, at brancheforeninger eller andre organer, som repræsenterer andre kategorier af private dataansvarlige, i samarbejde med Datatilsynet kan udarbejde adfærdskodekser, der skal bidrage til en korrekt anvendelse af reglerne i denne lov.

Om § 74 fremgår det af forarbejderne til persondataloven[663], at der ikke af bestemmelsen følger en forpligtelse til at udarbejde (ikke-bindende) adfærdskodekser. Endvidere fremgår det, at bestemmelsen således alene er indsat for i overensstemmelse med direktivets artikel 27 at tilskynde brancheforeninger mv. til at tage initiativ til, at der i samarbejde med Datatilsynet udarbejdes et sæt etiske regler på deres område. For så vidt angår de tilfælde hvor der udarbejdes adfærdskodekser, fremgår det tillige af bemærkningerne, at det forudsættes, at Datatilsynet påser, at et sådan sæt regler ikke er i uoverensstemmelse med reglerne i loven samt regler udstedt i medfør heraf. Herudover fremgår det, at Datatilsynet, hvis tilsynet finder det nødvendigt, kan indhente bemærkninger til udarbejdede udkast hos de registrerede eller deres repræsentanter.

Som nævnt ovenfor har persondatalovens § 74 sin baggrund i databeskyttelsesdirektivets artikel 27.

Af artikel 27, stk. 1, fremgår det om adfærdskodekser, at medlemsstaterne og Kommissionen tilskynder til udarbejdelsen af sådanne, der afhængigt af de særlige forhold i de forskellige sektorer skal bidrage til en korrekt anvendelse af de nationale bestemmelser, medlemsstaterne vedtager til gennemførelse af dette direktiv.

Om forelæggelse af adfærdskodekser for tilsynsmyndighederne fremgår det af artikel 27, stk. 2, 1. afsnit, at medlemsstaterne fastsætter bestemmelser om, at de brancheforeninger

[663] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00.

eller andre organer, som repræsenterer andre kategorier af dataansvarlige, som har udarbejdet udkast til nationale adfærdskodekser, eller som agter at ændre eller forlænge gældende nationale kodekser, skal kunne forelægge dem for den nationale myndighed til udtalelse.

Af artikel 27, stk. 2, 2. afsnit, fremgår det om kontrol af adfærdskodekser, at medlemsstaterne fastsætter bestemmelser om, at den nationale myndighed bl.a. skal kontrollere, at de udkast, den får forelagt, er i overensstemmelse med de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv. Endvidere fremgår det, at myndigheden, hvis den finder det hensigtsmæssigt, kan indhente bemærkninger fra de registrerede eller disses repræsentanter.

Om såkaldte EU-kodekser fremgår det af artikel 27, stk. 3, at udkast til EU-kodeks og forslag til ændring eller forlængelse af eksisterende EU-kodekser kan forelægges for Artikel 29-gruppen. Det fremgår endvidere om forelæggelse for Artikel 29-gruppen, at denne bl.a. udtaler sig om, hvorvidt de udkast, den har fået forelagt, er i overensstemmelse med de nationale bestemmelser til gennemførelse af dette direktiv. Herudover fremgår det, at Artikel 29-gruppen, hvis den finder det nødvendigt, kan indhente bemærkninger fra de registrerede eller disses repræsentanter. Endelig fremgår det, at Kommissionen kan tilse, at de kodekser, som gruppen har godkendt, offentliggøres på passende vis.

Herudover fremgår det af databeskyttelsesdirektivets præambelbetragtning nr. 61, at medlemsstaterne og Kommissionen inden for deres respektive kompetenceområder skal opfordre de berørte erhvervskredse til at udarbejde adfærdskodekser med henblik på, under hensyn til de særlige former for behandling, der udføres i bestemte sektorer, at fremme iværksættelsen af dette direktiv under overholdelse af de bestemmelser, medlemsstaterne har truffet til gennemførelse deraf.

5.22.2.2. Artikel 29-gruppens udtalelse af 10. september 1998 om proceduren for behandling af EU-adfærdskodekser i arbejdsgruppen (WP 13)

I ovennævnte udtalelse har Artikel 29-gruppen udtalt sig om, hvilken procedure arbejdsgruppen vil benytte, hvis en interesseret part – i medfør af databeskyttelsesdirektivets artikel 27, stk. 3 – vælger at forelægge et udkast til EU-adfærdskodeks for gruppen.

Om regler for forelæggelse og accept af adfærdskodekser, der behandles i arbejdsgruppen udtaler Artikel 29-gruppen i udtalelsens artikel 2, at:

”2.1 Udkast til adfærdskodeks kan forelægges arbejdsgruppen til behandling af enhver organisation, der er repræsentativ for den implicerede sektor, og som er etableret eller aktiv i et større antal medlemsstater.

2.2 Sådanne udkast til adfærdskodeks skal forberedes omhyggeligt, helst i samråd med de implicerede registrerede eller deres repræsentanter, og skal klart angive, hvilken organisation eller sektor kodeksen tilsigter at finde anvendelse på.

2.3 Udkast til adfærdskodeks skal affærdiges på et EU-sprog ledsaget af en oversættelse til engelsk og fransk og stiles til arbejdsgruppens formand via sekretariatet (Kommissionen, GD XV/D/1) og skal være ledsaget af en begrundelse.

2.4 Ufærdige udkast og udkast til adfærdskodeks, der ikke opfylder ovennævnte kriterier (kriterierne i punkt 2.1-2.3), vil ikke blive accepteret til behandling i arbejdsgruppen.

2.5 Sekretariatet anerkender modtagelsen af udkast til adfærdskodeks over for den forelæggende part.

2.6 I samråd med formanden udarbejder sekretariatet en rapport, der fastslår, om det forelagte udkast til adfærdskodeks opfylder kriterierne for accept i punkt 2.1–2.3.

2.7 Formanden afgør, om et forelagt udkast til adfærdskodeks opfylder kriterierne for accept. Finder formanden, at kriterierne ikke er opfyldt, informerer han medlemmerne af arbejdsgruppen og fastsætter en frist for reaktioner. Medmindre to eller flere medlemmer anmoder om, at spørgsmålet drøftes på det næste møde i arbejdsgruppen, meddeles formandens afgørelse den forelæggende part med en begrundelse for afvisningen af udkastet.”

Herudover udtaler Artikel 29-gruppen – i udtalelsens artikel 3 – om regler for udarbejdelse af arbejdsgruppens udtalelse, at:

”3.1 Forelagte udkast til adfærdskodeks, der opfylder kriterierne for accept, sendes til medlemmerne af arbejdsgruppen.

3.2 I samråd med formanden udarbejder sekretariatet forslag til udarbejdelse af en udtalelse, som drøftes i arbejdsgruppen. Sådanne forslag:

- kan slå til lyd for, at der nedsættes særlige arbejdsgrupper eller taskforcer, der består af et eller flere medlemmer af arbejdsgruppen og støttes af sekretariatet

- kan slå til lyd for, at der benyttes en forenklet procedure til behandling af en forelagt kodeks, især ved ændringer eller forlængelser af eksisterende kodekser, og

- rådgiver arbejdsgruppen om, hvorvidt og hvordan arbejdsgruppen bør søge at indhente synspunkter fra de implicerede registrerede eller deres repræsentanter eller andre parter.

3.3 I en første drøftelse af en forelagt kodeks fastslår arbejdsgruppen på grundlag af de forslag, der er omhandlet i artikel 3, punkt 3.2, hvilken procedure der skal benyttes i forbindelse med udtalelsen og dens udarbejdelse.

3.4 Udarbejdelsen af udtalelsen kan indebære, at der rettes henvendelse til den forelæggende part og andre interesserede parter for at indhente yderligere oplysninger eller få præciseret oplysninger eller for at drøfte nødvendige forbedringer i den forelagte kodeks, eventuelt med henblik på forelæggelse af et revideret udkast til kodeks.

3.5 Arbejdsgruppen kan give yderligere vejledning eller instrukser vedrørende udarbejdelsen af udtalelsen om en forelagt kodeks."

Endelig udtaler Artikel 29-gruppen – i udtalelsens artikel 4 – om regler vedrørende arbejdsgruppens udtalelse og meddelelsen af udtalelsen til de implicerede parter, at:

"4.1 Arbejdsgruppen afgør, om en forelagt adfærdskodeks:

- er i overensstemmelse med databeskyttelsesdirektiverne og, hvis dette er relevant, med de nationale bestemmelser, der er vedtaget til gennemførelse af disse direktiver

- er af tilstrækkelig høj kvalitet og viser indre sammenhæng og frembyder tilstrækkelig merværdi i forhold til direktiverne og anden gældende databeskyttelseslovgivning, især om udkastet til kodeks i tilstrækkelig grad fokuserer på de specifikke databeskyttelsesspørgsmål og -problemer, der findes i den organisation eller sektor, som kodeksen tilsigter at finde anvendelse på, samt anviser tilstrækkelig klare løsninger på disse spørgsmål og problemer.

4.2 Arbejdsgruppen underretter den forelæggende part og andre implicerede parter om sin udtalelse. Hvis arbejdsgruppen i udtalelsen afviser udkastet til kodeks, angives en begrundelse for denne afvisning.

4.3 Kommissionen kan sikre, at arbejdsgruppens udtalelser offentliggøres på passende vis."

5.22.2.3. Anvendelse af adfærdskodekser i praksis

5.22.2.3.1. Danske adfærdskodekser

Som nævnt ovenfor ses persondatalovens § 74 ikke at have haft praktisk betydning i Danmark, idet meget få brancheforeninger mv. har henvendt sig til Datatilsynet med et ønske om udarbejdelse af en adfærdskodeks.

I forhold til de få henvendelser om adfærdskodekser, der har været, ses ingen af dem at have resulteret i, at Datatilsynet har fundet, at udkastet til adfærdskodeks var i overensstemmelse med persondataloven.[664]

5.22.2.3.2. EU-adfærdskodekser

Artikel 29-gruppen ses kun i én udtalelse[665] at have udtalt, at en adfærdskodeks var i overensstemmelse med artikel 27 i databeskyttelsesdirektivet.

I sin udtalelse konkluderer Artikel 29-gruppen på side 6, at FEDMAs adfærdskodeks er i overensstemmelse og tilfører direktivet en tilstrækkelig merværdi ved i tilstrækkelig høj grad at fokusere på specifikke spørgsmål og problemer i forbindelse med direkte markedsføring og beskyttelse af personoplysninger, og at adfærdskodeksen tilbyder tilstrækkeligt klare løsninger på de relevante spørgsmål og problemer.

Det bemærkes, at Artikel 29-gruppen i en udtalelse af 13. juli 2010 (WP 174) er kommet med en opdateret udtalelse om FEDMAs europæiske adfærdskodeks for brug af personoplysninger i forbindelse med direkte markedsføring.

5.22.3. Databeskyttelsesforordningen

5.22.3.1. Forordningens artikel 40, stk. 1 – Tilskyndelse til udarbejdelse af adfærdskodekser

Af forordningens artikel 40, stk. 1, fremgår det, at medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen tilskynder til udarbejdelse af adfærdskodekser,

[664] Se f.eks. Datatilsynets j.nr. 2004-141-0002.

[665] Udtalelse af 13. juni 2003 om FEDMAs (Federation og European Marketing Associations) europæiske adfærdskodeks for brug af personoplysninger i forbindelse med direkte markedsføring.

der under hensyntagen til de særlige forhold i de forskellige behandlingssektorer og mikrovirksomheders og små og mellemstore virksomheders specifikke behov bidrager til korrekt anvendelse af denne forordning.

Af præambelbetragtning nr. 98 fremgår det endvidere, at sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, bør opfordres til at udarbejde adfærdskodekser inden for rammerne af denne forordning med henblik på at fremme en effektiv anvendelse af denne forordning under hensyntagen til de specifikke typer af behandling, der foretages i visse sektorer, og de særlige behov hos mikrovirksomheder og små og mellemstore virksomheder. Herudover fremgår det, at sådanne adfærdskodekser navnlig bør kunne justere dataansvarliges og databehandleres forpligtelser, så der tages hensyn til den risiko, som sandsynligvis vil følge af behandlingen for fysiske personers rettigheder og frihedsrettigheder.

Ved en sammenholdelse af forordningens artikel 40, stk. 1, med databeskyttelsesdirektivets artikel 27, stk. 1, kan det konstateres, at de to bestemmelser er næsten identiske. Ud over en tilføjelse af yderligere tilskyndende organer (tilsynsmyndighederne og Databeskyttelsesrådet) er det dog nyt, at der skal tages hensyn til bestemte virksomhedstypers særlige forhold, herunder mikrovirksomheder og små og mellemstore virksomheder. Dette skyldes formentlig, at der er et ønske om at hjælpe små virksomheder – der typisk ikke har en juridisk afdeling eller ressourcerne til at indhente ekstern juridisk rådgivning – til at efterleve forordningens regler gennem implementering af adfærdskodekser.

Når det i præambelbetragtning nr. 98, 2. punktum, anføres, at adfærdskodekser navnlig bør kunne justere dataansvarliges og databehandleres forpligtelser, så der tages hensyn til den risiko, som sandsynligvis vil følge af behandlingen for fysiske personers rettigheder og frihedsrettigheder, indebærer dette som noget nyt, at forordningens risikobaserede tilgang til databeskyttelse bliver inkluderet i adfærdskodekserne. Inkluderingen af forordningens risikobaserede tilgang i en adfærdskodeks fremgår ikke direkte af artikel 40, men såfremt en kodeks skal specificere anvendelsen af denne forordning, med hensyn til f.eks. artikel 24, 25 og 32 (Artikel 40, stk. 2, litra h), vil den risikobaserede tilgang formentlig blive en del af kodeksen, fordi det indgår som en del af artiklerne 24, 25 og 32.

Tilskyndelsen til udarbejdelse af adfærdskodekser fremgår også af listen over tilsynsmyndighedens opgaver i artikel 57, stk. 1, litra m, samt Databeskyttelsesrådets opgaver i artikel 70, stk. 1, litra n.

5.22.3.2. Forordningens artikel 40, stk. 2 – Udarbejdelse af adfærdskodekser

Det fremgår af forordningens artikel 40, stk. 2, at sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, kan udarbejde adfærdskodekser eller ændre eller udvide sådanne kodekser med henblik på at specificere anvendelsen af denne forordning, *såsom* med hensyn til:

a) rimelig og gennemsigtig behandling
b) de legitime interesser, som forfølges af den dataansvarlige i specifikke sammenhænge
c) indsamlingen af personoplysninger
d) pseudonymiseringen af personoplysninger
e) informationen, der gives til offentligheden og til registrerede
f) udøvelsen af registreredes rettigheder
g) informationen, der gives til børn, og beskyttelsen af børn og den måde, hvorpå samtykket fra indehavere af forældremyndighed over børn skal indhentes
h) foranstaltningerne og procedurerne omhandlet i artikel 24 og 25 og foranstaltningerne til at sikre behandlingssikkerhed som omhandlet i artikel 32
i) anmeldelsen af brud på persondatasikkerheden til tilsynsmyndighederne og underretningen af de registrerede om sådanne brud på persondatasikkerheden
j) overførslen af personoplysninger til tredjelande eller internationale organisationer, eller
k) udenretslige procedurer og andre procedurer for bilæggelse af tvister mellem dataansvarlige og registrerede vedrørende behandling, uden at det berører registreredes rettigheder i henhold til artikel 77 og 79.

Ovenstående liste er eksempler (grundet udtrykket "såsom") og dermed ikke som en udtømmende liste over, hvilke områder i forordningen der kan tages under behandling i en adfærdskodeks.

Af præambelbetragtning nr. 99 fremgår det tillige, at under udarbejdelsen af en adfærdskodeks eller i forbindelse med ændring eller udvidelse af en sådan kodeks, bør sammenslutninger og andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, høre relevante interessenter, herunder i muligt omfang registrerede, og tage hensyn til bemærkninger og synspunkter, der er fremsat som svar på sådanne høringer.

I modsætning til databeskyttelsesdirektivets artikel 27 og persondatalovens § 74 fremgår det ikke af forordningen, at en adfærdskodeks skal udarbejdes i *samarbejde med* tilsynsmyndigheden. Efter forordningen er tilsynsmyndighedens rolle således at afgive *udtalelser* og *eventuelt godkende* udkast til kodekser, som er udformet af andre.

Hverken i databeskyttelsesdirektivet eller i persondataloven oplistes der konkrete emner, som en adfærdskodeks kan specificere med henblik på anvendelsen af direktivet og persondataloven. Det er således nyt, når der i litra a-k ovenfor oplistes konkrete emner, som en adfærdskodeks kan specificere med henblik på anvendelsen af forordningen. Det må dog antages, at en adfærdskodeks efter gældende ret også vil kunne specificere de i forordningen nævnte emner, selvom det ikke er udtrykkeligt oplistet i direktivet eller i persondataloven.

Af artikel 40, stk. 2, fremgår det, at adfærdskodekser kan udarbejdes af sammenslutninger og andre organer, der repræsenterer *kategorier af* dataansvarlige eller databehandlere, mens direktivets artikel 27, stk. 2, peger på *brancheforeninger* og andre repræsentanter for *kategorier af* dataansvarlige. Der er altså i høj grad sammenfald med gældende ret på dette punkt. Når forordningen ikke udtrykkeligt viderefører begrebet "brancheforeninger", skyldes dette formentlig, at man har ønsket, at det skal stå mere åbent, hvem der kan udfærdige adfærdskodekser. Brancheforeninger er dog stadig oplagte kandidater til at udarbejde kodekser.

Med artikel 40, stk. 2, videreføres gældende ret i forhold til, at kodekser kan udarbejdes af organer, som repræsenterer *kategorier af* dataansvarlige. Nyt er det dog, at kodekser også kan udarbejdes af *kategorier af* databehandlere. Denne videreførelse af, at kodekser kan udarbejdes af kategorier af dataansvarlige (og nu også databehandlere) skyldes formentlig, at adfærdskodekser er nemmere at gennemføre i en gruppe af dataansvarlige (eller databehandlere), der har lignende behandlingsaktiviteter, hvorved de kan se en fælles fordel i en adfærdskodeks, og kan være fælles om opgaven med at udarbejde den.

Ved udarbejdelsen af en adfærdskodeks vil det næppe være tilstrækkeligt at have en generel viden om forordningen, it eller IT-sikkerhed. For at kunne skrive en kodeks, der f.eks. omhandler en bestemt behandlingsaktivitet indenfor sundhedsplejen, skal man således have indgående kendskab til netop denne behandlingsaktivitet, herunder i forhold til det daglige arbejde og de eventuelle usædvanlige arbejdssituationer, som behandlingsaktiviteterne måtte indgå i. Udarbejdes en kodeks af nogen, der ikke har denne *situationsnære* viden, er der en risiko for, at kodeksen måske nok overholder forordningen, men at den ikke vil fungere i praksis for sundhedspersonalet eller IT-personalet. En negativ sideeffekt af dette kan således være, at kodeksen ikke overholdes af sundhedspersonalet/IT-personalet i deres daglige arbejde, eller i de mere usædvanlige arbejdssituationer.

I lyset af ovennævnte må det ligeledes antages, at processen med at få et udkast til kodeks godkendt hos tilsynsmyndigheden og/eller Databeskyttelsesrådet vil være mere smidig, hvis udarbejdelsen af en adfærdskodeks sker i samarbejde mellem personer, der har *situa-*

tionsnær erfaring indenfor kodeksens genstand og personer, der har generel viden om forordningen og ekspertise indenfor IT-sikkerhed.

Et eksempel på, hvad en adfærdskodeks kunne have til formål at specificere anvendelsen af forordningen med hensyn til, kunne f.eks. være pseudonymisering af personoplysninger (artikel 40, stk. 2, litra d). Som en *hjælp til anvendelse af forordningen* – f.eks. sikkerhedskrav i artikel 32, stk. 1, litra a – kunne en sådan kodeks f.eks. angive, hvordan pseudonymisering skal udføres i praksis. Pseudonymisering er defineret i forordningen artikel 4, men kodeksen kan hjælpe med til at forklare, hvad der konkret skal til, før en specifik mængde data er ændret tilstrækkeligt til, at de kan omfattes af definitionen i artikel 4. Hvad der skal til for at pseudonymisere data afhænger af, hvilke ikke-pseudonymiserede data man starter ud med. Hvis data f.eks. indeholder oplysninger om navn og personnummer, er det formentlig ikke nok at fjerne personnummeret – det afhænger af muligheden for at knytte navnet til en fysisk person.

Eksemplet ovenover viser, at processen med pseudonymisering er meget afhængig af, hvilke ikke-pseudonymiserede data, man har til at begynde med. Dermed kan en konkret beskrivelse ikke passe til alle situationer og alle dataansvarlige og databehandlere, men beskrivelsen kan måske bringes til at passe til en mindre *sammenslutning af en bestemt kategori af dataansvarlige*, som alle foretager lignende databehandlinger på samme type ikke-pseudonymiserede data.

Hvis det fremgår af en adfærdskodeks, at der skal udføres pseudonymisering, og hvordan det skal udføres, giver det også mening, hvis det fremgår, *hvornår* pseudonymiseringen bør finde sted. Det kan således fremgå af kodeksen, at pseudonymisering skal ske så tidligt som muligt i arbejdsprocesserne, med henblik på at reducere antallet af personer, der arbejder med ikke-pseudonymiserede data. Det kræver en *situationsnær erfaring* at beskrive dette nærmere i en kodeks. En forudsætning herfor er, at man kender arbejdsprocesserne og ved, hvem der kan arbejde på pseudonymiserede data, og hvem der har brug for de ikke-pseudonymiserede data. Endvidere kan det fremgå af kodeksen, hvordan arbejdsprocesser bør indrettes/ændres, så færrest muligt kommer til at arbejde med ikke-pseudonymiserede data. Dette kan ligeledes kræve en situationsnær erfaring, idet man skal vide, hvordan arbejdsprocesserne kan indrettes, og hvilke problemer det kan skabe at ændre i eksisterende arbejdsprocesser.

Det fremgår ikke direkte af artikel 40, hvordan en kodeks bør udarbejdes. Dog fremgår det af præambelbetragtning nr. 99, at sammenslutninger og andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, bør høre relevante interessenter, herunder i muligt omfang registrerede, og tage hensyn til bemærkninger og synspunkter, der er

fremsat som svar på sådanne høringer, i forbindelse med udarbejdelsen af en adfærdskodeks eller i forbindelse med ændring eller udvidelse af en sådan kodeks. Høring af bl.a. de registrerede er også forudsat i databeskyttelsesdirektivets artikel 27, stk. 2, sidste punktum og artikel 27, stk. 3, 3. punktum, ligesom høring af de registrerede mv. også er omtalt i den ovenfor omtalte udtalelse af 10. september 1998 fra Artikel 29-gruppen. Efter direktivet er det dog tilsynsmyndigheden eller Artikel 29-gruppen, der skal foretage høringen. Dette ændres således med forordningen, men forordningen kan næppe antages at udelukke, at tilsynsmyndigheden kan foretage en høringsproces omkring et udkast til kodeks, hvor der indhentes bemærkninger fra de registrerede eller disses repræsentanter.

Det må antages, at inddragelse af registrerede og andre interessenter vil øge kvaliteten af en adfærdskodeks. F.eks. vil registrerede og interessenter, herunder organisationer der har fokus på patienters forhold og rettigheder, formentlig kunne hjælpe med at afdække relevante aspekter og risici i forhold til en specifik behandlingsaktivitet i sundhedssektoren. Inddragelse af sådanne relevante interessenter vil formentlig også kunne øge sandsynligheden for, at en kodeks vil blive godkendt af tilsynsmyndighederne, Databeskyttelsesrådet eller Kommissionen.

Overholdelse af adfærdskodekser skal i øvrigt også inddrages ved vurderingen af konsekvenserne af de behandlingsaktiviteter, der udføres af de pågældende dataansvarlige eller databehandlere, navnlig i forbindelse med en konsekvensanalyse vedrørende databeskyttelse, jf. artikel 35, stk. 8. Dette underbygger yderligere behovet for at inddrage registrerede og interessenter i arbejdet med en adfærdskodeks, når disse kan hjælpe med at afdække relevante risici.

5.22.3.3. Forordningens artikel 40, stk. 3 – Overførsel af oplysninger til tredjelande og internationale organisationer

Af forordningens artikel 40, stk. 3, fremgår det, at adfærdskodekser, der er godkendt i henhold til artikel 40, stk. 5, og er generelt gyldige i henhold til artikel 40 stk. 9 – ud over overholdelse af de dataansvarlige eller databehandlere, der er omfattet af denne forordning – også kan overholdes af dataansvarlige eller databehandlere, der i henhold til artikel 3 om det territoriale anvendelsesområde *ikke* er omfattet af denne forordning, med henblik på at sikre fornødne garantier inden for rammerne af overførsel af personoplysninger til tredjelande eller internationale organisationer, jf. artikel 46, stk. 2, litra e. Det fremgår endvidere, at sådanne dataansvarlige eller databehandlere, gennem kontrakter eller andre retligt bindende instrumenter, skal afgive bindende tilsagn, som kan håndhæves, om at anvende disse fornødne garantier, herunder for så vidt angår registreredes rettigheder.

5.22.3.4. Forordningens artikel 40, stk. 4 – Mekanismer til kontrol af overholdelse
Det fremgår af forordningens artikel 40, stk. 4, at en adfærdskodeks omhandlet i artikel 40, stk. 2, *skal* indeholde mekanismer, der sætter organet omhandlet i artikel 41, stk. 1, i stand til at foretage obligatorisk kontrol for at sikre, at den dataansvarlige eller databehandler, der påtager sig at anvende adfærdskodeksen, overholder dens bestemmelser, uden at dette berører opgaverne og beføjelserne for de tilsynsmyndigheder, der er kompetente i henhold til artikel 55 eller 56.

Der henvises til afsnit 5.23. om kontrol af godkendte adfærdskodekser.

Forordningens artikel 40, stk. 4, indebærer således, at en adfærdskodeks ikke må være formuleret på en sådan måde, at det i praksis er umuligt at kontrollere, om den overholdes eller ej. Dette må bl.a. indebære, at kodeksen ikke må være ukonkret eller tvetydig.

Hvilke *mekanismer*, der kan muliggøre en *kontrol af*, om adfærdskodeksen overholdes, er meget afhængig af kodeksens genstand.

Hvis en adfærdskodeks f.eks. indeholder et krav om, at en hjemmeside, der behandler persondata (udvekslet med brugeren), skal sikres imod ondsindede angreb, skal kodeksen indeholde *mekanismer*, der muliggør *kontrol af*, om dette krav efterleves. Eksempler på sådanne *mekanismer* kunne være, hvis kodeksen indeholder krav om, at hjemmesiden jævnligt skal udsættes for sårbarhedstests[666] og penetrationstests[667], og at der skal handles på resultatet af sådanne tests, så fundne sårbarheder straks elimineres. Kodeksen kan endvidere indeholde krav om dokumentation af de udførte tests, ændringer til programkode, og en gentaget test til bekræftelse af, at sårbarhederne er elimineret. En mekanisme kunne også være, at kontrolorganet skal have mulighed for at få udført sårbarhedstests/penetrationstests, hvorved den reelle effekt af gennemførte foranstaltninger kan bekræftes – altså om de fundne sårbarheder vitterligt er elimineret. Ovennævnte *mekanismer* kan muliggøre en konkret *kontrol af,* om det specifikke krav ("hjemmesiden skal sikres imod ondsindede angreb") kan anses for overholdt.

Mekanismer kan også tilsigte at sikre, at den dataansvarlige ikke kan hindre en fornøden kontrol af, at en adfærdskodeks overholdes. Hvis en dataansvarlig f.eks. kræver fire ugers varsel, inden en kontrol kan udføres, kan det måske betragtes som en hindring, hvis perioden på fire uger kan udnyttes af den dataansvarlige til at skjule manglende overholdelse af

[666] En test der søger at afdække sårbarheder i software - sårbarheder som kan udnyttes af ondsindede til at kompromittere datas integritet, fortrolighed eller tilgængelighed. Dette er typisk det første skridt i en penetrationstest.
[667] En test der vurderer et IT-systems beskyttelse mod forskellige typer af angreb.

kodeksen. Til at imødegå dette kan en kodeks indeholde et krav (*mekanisme)* om, at kontrollen skal kunne udføres uden varsel. En alternativ *mekanisme* kunne være at kræve dokumentation, som ikke kan ændres af den dataansvarlige med bagudrettet virkning, således at det ikke har betydning, om kontrollen sker med eller uden varsel.

Når en adfærdskodeks skal indeholde så specifikke krav og mekanismer, skal der også specifik viden til for at kunne vurdere, hvilke krav og mekanismer der er nødvendige. Dette stiller krav til specifik viden og erfaring hos både kontrolorganet (efter forordningens artikel 41), men også tilsynsmyndigheden, da denne skal afgive udtalelse om og godkende udkast til adfærdskodekser i medfør af forordningens artikel 40, stk. 5, jf. mere herom nedenfor.

5.22.3.5. Forordningens artikel 40, stk. 5 – Forelæggelse af kodeks for tilsynsmyndigheden til godkendelse

Af forordningens artikel 40, stk. 5, fremgår det, at sammenslutninger og andre organer omhandlet i artikel 40, stk. 2, der har til hensigt at udarbejde en adfærdskodeks eller at ændre eller udvide en eksisterende adfærdskodeks, kan forelægge et udkast til kodeks, ændring eller udvidelse for den tilsynsmyndighed, der er kompetent i henhold til artikel 55. Det fremgår desuden, at tilsynsmyndigheden afgiver udtalelse om, hvorvidt udkastet til adfærdskodeks, ændring eller udvidelse overholder denne forordning, og godkender dette udkast til kodeks, ændring eller udvidelse, hvis den finder, at kodeksen sikrer tilstrækkelige fornødne garantier.

Afgivelse af udtalelser om og godkendelse af adfærdskodekser fremgår også af listen over tilsynsmyndighedens opgaver, artikel 57, stk. 1, litra m, ligesom det fremgår af artikel 58, stk. 3, litra d, at tilsynsmyndigheden har beføjelse til at afgive udtalelse og godkende forslag til adfærdskodekser i henhold til artikel 40, stk. 5.

Efter artikel 40, stk. 5, har tilsynsmyndigheden således pligt til at udtale sig om, hvorvidt et forelagt udkast til adfærdskodeks overholder forordningen, ligesom tilsynsmyndigheden har pligt til at godkende udkastet til kodeks, hvis kodeksen sikrer tilstrækkelige fornødne garantier.

I forhold til gældende ret er det nyt, at tilsynsmyndigheden også har en pligt til at godkende et udkast til adfærdskodeks, hvis kodeksen sikrer tilstrækkelige fornødne garantier.

Tilsynsmyndighedens godkendelse af en adfærdskodeks afhænger efter artikel 40, stk. 5, af en vurdering af, hvorvidt adfærdskodeksen sikrer tilstrækkelige fornødne garantier. Ved denne vurdering må tilsynsmyndigheden bl.a. se på, om en kodeks er dækkende i forhold

til det begrænsede område, som er kodeksens genstand, ligesom tilsynsmyndigheden må se på, om kodeksen indeholder mekanismer, der sætter kontrolorganet i stand til at foretage kontrol af overholdelsen af kodeksens bestemmelser.

Der kan umiddelbart være tre udfald af tilsynsmyndighedens gennemgang af et forelagt udkast til adfærdskodeks.

For det første kan tilsynsmyndighedens gennemgang føre til, at tilsynsmyndigheden udtaler, at udkastet til adfærdskodeks overholder forordningen, og at adfærdskodeksen sikrer tilstrækkelige fornødne garantier, hvormed adfærdskodeksen kan godkendes.

For det andet kan tilsynsmyndighedens gennemgang føre til, at tilsynsmyndigheden udtaler, at udkastet til adfærdskodeks ikke overholder forordningen, og/eller at adfærdskodeksen ikke sikrer tilstrækkelige fornødne garantier, hvormed adfærdskodeksen ikke kan godkendes.

Endelig kan tilsynsmyndighedens gennemgang for det tredje føre til, at tilsynsmyndigheden konkluderer, at udkastet til adfærdskodeks vedrører behandlingsaktiviteter i flere medlemsstater, hvorfor udkastet til adfærdskodeks skal forelægges for Databeskyttelsesrådet til udtalelse (efter proceduren i artikel 63 om sammenhængsmekanisme), inden udkastet kan godkendes.

I de situationer, hvor et udkast til adfærdskodeks ikke kan godkendes, vil tilsynsmyndigheden skulle begrunde, hvorfor dette er tilfældet. En pligt dertil følger formentlig allerede af kravet i artikel 40, stk. 5, om, at tilsynsmyndigheden skal komme med en udtalelse, men følger også af de almindelige begrundelsesregler i forvaltningsloven. En dataansvarlig, der har fået en negativ udtalelse, har således mulighed for efterfølgende at tage højde for tilsynsmyndighedens udtalelse, inden et eventuelt nyt udkast forelægges for tilsynsmyndigheden.

Det skal i den forbindelse bemærkes, at tilsynsmyndigheden formentlig sjældent vil blive "tvunget" til at komme med en egentlig negativ udtalelse om et udkast til adfærdskodeks. Dette skyldes, at det må antages, at den sammenslutning eller lignende, der forelægger et udkast, og tilsynsmyndigheden vil være i en dialog om udkastet undervejs, så eventuelle problematikker kan blive afhjulpet. Efter forordningens artikel 57, stk. 1, litra d, skal en tilsynsmyndighed f.eks. også fremme dataansvarliges og databehandleres kendskab til deres forpligtelser efter forordningen. Tilsynsmyndigheden har således en rådgivningsforpligtelse.

5.22.3.6. Forordningens artikel 40, stk. 6 – Offentliggørelse af kodeks ved tilsynsmyndigheden

Efter forordningens artikel 40, stk. 6, skal tilsynsmyndigheden, hvis udkastet til kodeks eller ændring eller udvidelse godkendes i overensstemmelse med stk. 5, og hvis den pågældende adfærdskodeks ikke vedrører behandlingsaktiviteter i flere medlemsstater, registrere og offentliggøre kodeksen.

5.22.3.7. Forordningens artikel 40, stk. 7 – Forelæggelse af kodeks for Databeskyttelsesrådet

Det fremgår af forordningens artikel 40, stk. 7, at hvis et udkast til adfærdskodeks vedrører behandlingsaktiviteter i flere medlemsstater, skal den tilsynsmyndighed, der er kompetent i henhold til artikel 55, inden godkendelsen af udkastet til kodeks, ændring eller udvidelse, efter proceduren i artikel 63 forelægge udkastet for Databeskyttelsesrådet, der afgiver en udtalelse om, hvorvidt udkastet til kodeks, ændring eller udvidelse overholder denne forordning eller sikrer fornødne garantier i den situation, der er omhandlet i artikel 40, stk. 3.

Efter forordningens artikel 40, stk. 7, har *tilsynsmyndigheden* således pligt til at forelægge et udkast til adfærdskodeks for Databeskyttelsesrådet til udtalelse, hvis kodekset vedrører behandlingsaktiviteter i flere medlemsstater.

Umiddelbart kan det være svært for tilsynsmyndigheden at vurdere, om en adfærdskodeks vedrører behandlingsaktiviteter i flere medlemsstater. Der vil således kunne være et behov for, at tilsynsmyndigheden indhenter information herom fra de involverede dataansvarlige og/eller databehandlere, hvis det ikke allerede fremgår af det indsendte materiale.

I lyset heraf vil det formentlig forkorte tilsynsmyndighedens sagsbehandlingstid, hvis den sammenslutning af dataansvarlige eller databehandlere, som udarbejder et udkast til kodeks, selv adresserer spørgsmålet om, hvorvidt kodekset vedrører behandlingsaktiviteter i flere medlemsstater. Det bør endvidere fremgå af kodeksen, hvis den ikke kan anvendes ved behandlingsaktiviteter i flere medlemsstater.

Hvis et udkast til adfærdskodeks vedrører behandlingsaktiviteter i flere medlemsstater, *skal* Databeskyttelsesrådet afgive en udtalelse jf. artikel 64, stk. 1, litra b, inden kodeksen kan godkendes af tilsynsmyndigheden. En eventuelt efterfølgende godkendelse fra tilsynsmyndigheden må naturligvis forudsætte, at Databeskyttelsesrådet kommer frem til, at udkastet overholder forordningen eller sikrer fornødne garantier.

5.22.3.8. Forordningens artikel 40, stk. 8 – Orientering af Kommissionen
Af forordningens artikel 40, stk. 8, fremgår det, at hvis den i stk. 7 omhandlede udtalelse bekræfter, at udkastet til kodeks, ændring eller udvidelse overholder denne forordning eller sikrer fornødne garantier i den situation, der er omhandlet i stk. 3, indsender Databeskyttelsesrådet sin udtalelse til Kommissionen.

5.22.3.9. Forordningens artikel 40, stk. 9 – Generel gyldighed i unionen
Det fremgår af forordningens artikel 40, stk. 9, at Kommissionen ved hjælp af gennemførelsesretsakter kan afgøre, at den godkendte adfærdskodeks, ændring eller udvidelse, som den har modtaget (fra Databeskyttelsesrådet) i henhold til stk. 8, generelt er gyldig i Unionen. Endvidere fremgår det, at disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 92, stk. 2.

Bestemmelsen i artikel 40, stk. 9, indebærer f.eks., at Kommissionen kan afgøre, at en adfærdskodeks (f.eks. omhandlende behandlingssikkerhed og efterlevelse af artikel 32), der oprindeligt blev forelagt for en udenlandsk tilsynsmyndighed, f.eks. i Tyskland, skal have gyldighed i alle medlemsstater, inklusiv Danmark.

På denne baggrund må det også antages, at dataansvarlige og databehandlere i Danmark med tiden kan vælge at følge adfærdskodekser, som er udarbejdet i et andet EU-land, og som er gjort generelt gyldige i Unionen af Kommissionen.

Artikel 40, stk. 9, omtaler ikke den situation, hvor Kommissionen måtte vælge ikke at afgøre, at en adfærdskodeks skal have gyldighed i alle medlemsstater. I disse situationer vil kodeks kun kunne benyttes i de enkelte medlemsstater, når der er indhentet en godkendelse efter artikel 40, stk. 5, fra tilsynsmyndigheden. En sådan godkendelse burde dog være en formalitet, når Databeskyttelsesrådet er kommet med en positiv udtalelse om kodeks.

5.22.3.10. Forordningens artikel 40, stk. 10 – Offentliggørelse af kodekser med generel gyldighed i unionen
Af forordningens artikel 40, stk. 10, fremgår det, at Kommissionen tilser, at de godkendte kodekser, som i henhold til Kommissionen har generel gyldighed, jf. stk. 9, offentliggøres på passende vis.

5.22.3.11. Forordningens artikel 40, stk. 11 – Offentliggørelse af alle kodekser ved Databeskyttelsesrådet

Ifølge forordningens artikel 40, stk. 11, skal Databeskyttelsesrådet samle alle godkendte adfærdskodekser, ændringer og udvidelser i et register og gøre dem offentligt tilgængelige på passende vis.

Bestemmelsen i forordningens artikel 40, stk. 11, er i modsætning til bestemmelsen i stk. 10 ikke begrænset til adfærdskodekser, der er generelt gyldige i unionen. Databeskyttelsesrådet skal således muligvis også registrere og offentliggøre de kodekser, som i henhold til stk. 6 registreres og offentliggøres af de enkelte tilsynsmyndigheder.

5.22.3.12. Samspillet mellem artikel 40 og andre bestemmelser i forordningen

5.22.3.12.1. Samspillet med artikel 24 – Den dataansvarliges ansvar

Efter forordningens artikel 24, stk. 3, kan overholdelse af godkendte adfærdskodekser bruges som et element til at påvise overholdelse af den dataansvarliges forpligtelser i henhold til forordningen, jf. også artikel 5, stk. 2.

5.22.3.12.2. Samspillet med artikel 28 – Databehandlers påvisning af fornødne garantier

Efter forordningens artikel 28, stk. 5, kan en databehandlers overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 bruges som et element til at påvise fornødne garantier som omhandlet i artikel 28, stk. 1 og 4.

Dette omfatter således databehandleres garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandling opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder.

5.22.3.12.3. Samspillet med artikel 32 – Behandlingssikkerhed

Af forordningens artikel 32, stk. 3, fremgår det, at overholdelse af en godkendt adfærdskodeks, som omhandlet i artikel 40, kan bruges som et element til at påvise den dataansvarliges og databehandlerens overholdelse af kravene til behandlingssikkerhed i artikel 32, stk. 1.

5.22.3.12.4. Samspillet med artikel 35 – Konsekvensanalyse vedrørende databeskyttelse

Det fremgår af forordningens artikel 35, stk. 8, at overholdelse af godkendte adfærdskodekser skal inddrages behørigt ved vurderingen af konsekvenserne af de databehandlingsaktiviteter, der udføres af de pågældende dataansvarlige eller databehandlere, navnlig i forbindelse med en konsekvensanalyse vedrørende databeskyttelse.

I præambelbetragtning nr. 77 præciseres det i forhold til ovennævnte, at adfærdskodekser kan spille en rolle i den dataansvarliges eller databehandleres identificering af risici, og vurdering af risicis oprindelse, karakter, sandsynlighed og alvor, samt om identificering af bedste praksis med henblik på at begrænse risici.

5.22.3.12.5. Samspillet med artikel 46 – Overførsler omfattet af fornødne garantier
Af forordningens artikel 46, stk. 2, litra e, fremgår det, at de fornødne garantier i forbindelse med overførsel af personoplysninger til et såkaldt usikkert tredjeland – uden krav om specifik godkendelse fra en tilsynsmyndighed – kan sikres gennem en godkendt adfærdskodeks i medfør af artikel 40 sammen med bindende tilsagn, som kan håndhæves, fra den dataansvarlige eller databehandleren i tredjelandet om at anvende de fornødne garantier, herunder vedrørende registreredes rettigheder.

5.22.3.12.6. Samspillet med artikel 83 – Administrative bøder
Af forordningens artikel 83, stk. 2, litra j, fremgår det, at der ved afgørelsen af, hvorvidt der skal pålægges en administrativ bøde, og om den administrative bødes størrelse i hver enkelt sag, skal tages behørigt hensyn til, om godkendte adfærdskodekser er overholdt.

Overholdelse af en godkendt adfærdskodeks i forbindelse med en given behandling vil således f.eks. kunne inddrages som en formildende omstændighed ved fastsættelsen af en eventuel bødes størrelse.

Det er i den forbindelse vigtigt at være opmærksom på, at overholdelse af en kodeks ikke i sig selv er bevis på overholdelse af forordningen, heller ikke for så vidt angår specifikke artikler i forordningen, som kodeksen måtte specificere anvendelsen af forordningen i forhold til. Overholdelse af en kodeks kan dermed heller ikke fritage en dataansvarlig eller databehandler for ansvar, hvorfor det heller ikke antages, at en bøde helt kan frafaldes alene med baggrund i overholdelse af en godkendt adfærdskodeks.

5.22.4. Overvejelser
Med forordningen bliver reglerne om adfærdskodekser mere detaljerede og begrænser sig – i modsætning til persondataloven – ikke nødvendigvis til private dataansvarlige. Der er med artikel 40 i vidt omfang tale om en nyskabelse i forhold til gældende ret.

Da kodekser nævnes i flere artikler om behandlingssikkerhed og den potentielt positive effekt det kan have på administrative bøder, har kodekser potentiale til at få større betydning fremover.

Af forordningens artikel 40, stk. 1, er det nyt i forhold til gældende ret, at der skal tages hensyn til bestemte virksomhedstypers særlige forhold, herunder mikrovirksomheder og små og mellemstore virksomheder. Derudover er det nyt, at forordningens risikobaserede tilgang til databeskyttelse kan blive inkluderet i adfærdskodekserne som følge af forordningens artikler 24, 25 og 32.

Det følger af forordningens artikel 40, stk. 2, at tilsynsmyndighedens rolle er at afgive udtalelser og eventuelt godkende udkast til kodekser, hvilket er en ændring i forhold til gældende ret, hvor en adfærdskodeks skal udarbejdes i samarbejde med tilsynsmyndigheden. Derudover tilføjer bestemmelsen som noget nyt en oplistning af konkrete emner i litra a–k, som en adfærdskodeks kan specificere med henblik på anvendelsen af forordningen. Det er endvidere nyt, at kodekser også kan udarbejdes af kategorier af databehandlere. Endelig er det nyt, at det forudsættes, at dataansvarlige eller databehandlere foretager en høring af relevante interessenter.

Det følger som noget nyt af forordningens artikel 40, stk. 5, at tilsynsmyndigheden har en pligt til at godkende et udkast til adfærdskodeks, hvis kodeksen sikrer tilstrækkelige fornødne garantier.

Derudover er tilsynsmyndighedens pligt til at forelægge en adfærdskodeks for Databeskyttelsesrådet til udtalelse, hvis kodekset vedrører behandlingsaktiviteter i flere medlemsstater, efter forordningens artikel 40, stk. 7, en nydannelse i forhold til gældende ret. Også Databeskyttelsesrådets efterfølgende fremsendelse af sin udtalelse til Kommissionen efter forordningens artikel 40, stk. 8, er en nydannelse. Endelig er det nyt i forhold til gældende ret, at Kommissionen efter proceduren i artikel 40, stk. 9, ved hjælp af en gennemførelsesretsakt kan afgøre, at en adfærdskodeks opnår generel gyldighed i Unionen.

5.23. Kontrol af godkendte adfærdskodekser, artikel 41

5.23.1. Præsentation

Efter databeskyttelsesforordningens artikel 40 skal medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen tilskynde til udarbejdelse af adfærdskodekser, der under hensyntagen til de særlige forhold i de forskellige behandlingssektorer og mikrovirksomheders og små og mellemstore virksomheders specifikke behov bidrager til korrekt anvendelse af forordningen.

Adfærdskodekser vil således kunne benyttes til at lette dataansvarliges og databehandleres overholdelse af krav i forordningen.

En forudsætning for, at en adfærdskodeks kan benyttes af dataansvarlige og databehandlere til at implementere forordningen er dog, at de pågældende dataansvarlige og databehandlere overholder adfærdskodeksen i praksis.

Der er således et behov for, at der føres kontrol med, at godkendte adfærdskodekser overholdes i praksis, hvilket forordningens artikel 41 fastsætter nærmere regler for. Dog finder disse regler ikke anvendelse på behandlinger, der udføres af offentlige myndigheder og organer.

5.23.2. Gældende ret

Der findes ingen regler om kontrol af godkendte adfærdskodekser i hverken databeskyttelsesdirektivet eller i persondataloven.

5.23.3. Databeskyttelsesforordningen

5.23.3.1. Forordningens artikel 41, stk. 1 – Kontrol af overholdelsen af en kodeks

Af forordningens artikel 41, stk. 1, fremgår det, at kontrol af overholdelsen af en adfærdskodeks i henhold til artikel 40 *kan* foretages af et organ, der har et passende ekspertiseniveau for så vidt angår kodeksens genstand, og som er akkrediteret til dette formål af den kompetente tilsynsmyndighed, uden at dette berører den kompetente tilsynsmyndigheds opgaver og beføjelser i henhold til artikel 57 og 58.

Når overladelse af kontrollen med overholdelsen af en adfærdskodeks ikke berører den kompetente tilsynsmyndigheds opgaver og beføjelser, betyder dette bl.a., at tilsynsmyndigheden stadig har sine opgaver og beføjelser for så vidt angår behandlingsaktiviteter, der foregår i tilknytning til en adfærdskodeks, som kontrolleres af et akkrediteret organ. Tilsynsmyndigheden kan dermed f.eks. stadig føre tilsyn med behandlingsaktiviteter, både generelt og i forhold til eventuelle specifikke områder, som måtte være kodeksens genstand.

Som artikel 41, stk. 1, er formuleret, fremgår det, at kontrol med overholdelsen af en kodeks *kan* foretages af et kontrolorgan, men at det ikke er et krav. Formuleringen af stk. 1 er formentlig begrundet i, at det fremgår af artikel 41, stk. 6, at artikel 41 ikke finder anvendelse på behandling, der udføres af offentlige myndigheder og organer. Kontrol med overholdelsen af en kodeks i offentlige myndigheder og organer foretages altså ikke af kontrolorganet. Det er vigtigt at være opmærksom på, at tilsynsmyndigheden fører tilsyn med *overholdelse af forordningen,* og kontrolorganet fører kontrol med *overholdelse af en adfærdskodeks*. Tilsynsmyndighedens kan dog føre tilsyn med et område, der efter den dataansvarliges opfattelse er dækket af en adfærdskodeks, og i den situation, kan tilsynsmyn-

dighedens tilsyn afsløre mangler og dermed manglende efterlevelse af kodeksen, på samme måde som hvis der var udført en kontrol ved et kontrolorgan.

Artikel 41 indeholder ikke et krav om, at der akkrediteres et kontrolorgan, men opgaven med at føre kontrol med overholdelsen af en adfærdskodeks er modsætningsvist ikke en del af tilsynsmyndighedens opgaver, jf. artikel 57.

En situation med et manglende kontrolorgan kan f.eks. opstå, hvis kun ét organ er akkrediteret til at kontrollere overholdelse af en specifik kodeks, og dette organ mister sin akkreditering, jf. artikel 41, stk. 7. Dette vil efterlade den allerede godkendte adfærdskodeks uden et tilhørende kontrolorgan. Eksistensen af et akkrediteret kontrolorgan efter artikel 41 er ikke en gyldighedsbetingelse for en adfærdskodeks, godkendt efter proceduren i artikel 40. Den godkendte kodeks kan i den forbindelse stadig bruges til at lette den praktiske implementering af forordningen, men den kan næppe påberåbes i forhold til efterlevelse af forordningen, hvis der ikke sker kontrol af, om kodeksen overholdes.

Overholdelse af en kodeks kan i følge artikel 24 bruges som element til at påvise overholdelse af den dataansvarliges forpligtelser i henhold til forordningen. Dette må som nævnt nok forudsætte, at der faktisk foretages kontrol deraf.

Kontrol med overholdelse af en kodeks kan ende i suspension eller udelukkelse fra kodeksen og suspension eller udelukkelse indebærer, at en dataansvarlig eller en databehandler bl.a. ikke kan eller må anvende kodeksen som element til at påvise overholdelse af sine forpligtelser, jf. artikel 24, stk. 3.

5.23.3.2. Forordningens artikel 41, stk. 2 – Akkreditering af kontrolorgan
Det fremgår af forordningens artikel 41, stk. 2, at et organ som omhandlet i stk. 1 kan akkrediteres til at kontrollere overholdelsen af en adfærdskodeks, hvis dette organ har:

a) påvist sin uafhængighed og ekspertise for så vidt angår kodeksens genstand til den kompetente tilsynsmyndigheds tilfredshed

b) fastlagt procedurer, der gør det muligt for organet at vurdere dataansvarliges og databehandleres egnethed til at anvende kodeksen, kontrollere deres overholdelse af dens bestemmelser og regelmæssigt vurdere kodeksens virkemåde

c) fastlagt procedurer og ordninger for behandling af klager over overtrædelser af kodeksen eller den måde, hvorpå kodeksen er blevet eller bliver gennemført af en dataansvarlig eller

en databehandler, og at gøre disse procedurer og ordninger gennemsigtige for registrerede og offentligheden, *og*

d) påvist til den kompetente tilsynsmyndigheds tilfredshed, at dets opgaver og pligter ikke fører til en interessekonflikt.

Fælles for bestemmelserne i litra a-d er, at et organ, der ønsker at blive akkrediteret skal påvise og dokumentere en række nærmere oplistede ting over for tilsynsmyndigheden.

Tilsynsmyndigheden vil således også ved sin akkreditering af organet skulle efterse, at organet har fremlagt den fornødne dokumentation mv.

Henset til at adfærdskodekser kan dække meget forskellige brancher og mange typer af behandlingsaktiviteter, kan kriterier for akkreditering af et organ potentielt også være meget forskellige.

5.23.3.3. Forordningens artikel 41, stk. 3 – Forelæggelse af kriterier for Databeskyttelsesrådet

Af forordningens artikel 41, stk. 3, fremgår det, at den kompetente tilsynsmyndighed skal forelægge et udkast til kriterier for akkreditering af et organ som omhandlet i denne artikels stk. 1 for Databeskyttelsesrådet i henhold til sammenhængsmekanismen, der er omhandlet i artikel 63.

5.23.3.4. Forordningens artikel 41, stk. 4 – Suspension og udelukkelse fra kodeks

Det fremgår af forordningens artikel 41, stk. 4, at et organ som omhandlet i artikel 41, stk. 1 – uden at dette berører den kompetente tilsynsmyndigheds opgaver og beføjelser eller bestemmelserne i kapitel VIII – under forudsætning af fornødne garantier træffer de nødvendige foranstaltninger i tilfælde af en dataansvarligs eller databehandlers overtrædelse af kodeksen, herunder suspension eller udelukkelse af den dataansvarlige eller databehandleren fra kodeksen. Herudover fremgår det, at organet underretter den kompetente tilsynsmyndighed om sådanne foranstaltninger og begrundelsen for at have truffet dem.

Forordningen ses ikke at specificere, hvordan, hvornår eller med hvilket minimumsinterval det akkrediterede organ skal kontrollere dataansvarliges og databehandleres efterlevelse af en kodeks. Dette skyldes formentlig, at det kan variere meget fra adfærdskodeks til adfærdskodeks, hvordan, hvornår og med hvilket interval det er hensigtsmæssigt eller meningsfuldt, at der føres kontrol. Det må således vurderes i forhold til det konkrete kodeks.

Det er heller ikke nærmere specificeret, hvad der skal forstås ved, at organet skal træffe de nødvendige foranstaltninger *"under forudsætning af fornødne garantier"*. Det forekommer dog oplagt, at en fornøden garanti blandt andet kan være, at det akkrediterede organ skal høre den berørte dataansvarlige eller databehandler, inden der træffes fornødne foranstaltninger.

Når det akkrediterede organ kan træffe en foranstaltning, der består i en suspension af en dataansvarlig eller en databehandler, må det antages, at en sådan kan betyde, at en dataansvarlig eller en databehandler midlertidigt suspenderes fra adfærdskodeksen, med det resultat, at den pågældende dataansvarlige eller databehandler i en periode ikke kan eller må:

- Proklamere efterlevelse af kodeksen til f.eks. kunder,
- anvende kodeksen som element til at påvise overholdelse af sine forpligtelser, jf. artikel 24, stk. 3,
- anvende kodeksen som element til at påvise fornødne garantier som omhandlet i artikel 28, stk. 1 og 4,
- anvende kodeksen som element til at påvise overholdelse af kravene i artikel 32, stk. 1, eller
- anvende kodeksen som element til at påvise fornødne garantier i henhold til artikel 46, stk. 2, litra e.

I modsætning til en suspension vil en egentlig udelukkelse af en dataansvarlig eller en databehandler fra en adfærdskodeks ikke være af midlertidig karakter, men derimod af vedvarende karakter. Ovennævnte konsekvenser vil dog være de samme.

En suspension eller udelukkelse af en dataansvarlig eller en databehandler fra en adfærdskodeks vil også kunne få betydning for vurderingen af de databehandlingsaktiviteter, der udføres af de pågældende dataansvarlige eller databehandlere efter forordningens artikel 35, stk. 8, i forbindelse med en konsekvensanalyse vedrørende databeskyttelse. Denne problemstilling kan dog imødekommes ved, at det akkrediterede kontrolorgan skal underrette den kompetente tilsynsmyndighed om en dataansvarlig eller en databehandlers suspension eller udelukkelse fra en godkendt adfærdskodeks. På denne måde vil tilsynsmyndigheden f.eks. have mulighed for at igangsætte en undersøgelse af, hvilken betydning en suspension eller udelukkelse har for en tidligere udført konsekvensanalyse.

Idet konsekvensanalysen har betydning for den dataansvarliges eller databehandlerens opfyldes af bestemmelser i forordningen, og henset til bestemmelsen om ansvarlighed i artikel 5, stk. 2, skal den dataansvarlige eller databehandleren selv undersøge de afledte kon-

sekvenser af en suspension eller udelukkelse fra adfærdskodeksen, uanset om tilsynsmyndigheden ikke skulle igangsætte en undersøgelse på baggrund af en suspension eller udelukkelse.

Hvis en dataansvarlig eller databehandler har påvist overholdelse af kravene i dele af forordningen gennem anvendelse af en adfærdskodeks, kan en konstatering af manglende overholdelse af kodeksen også indikere manglende overholdelse af de samme dele af forordningen. I sådanne tilfælde kan det derfor også være relevant for tilsynsmyndigheden at overveje, om der skal foretages en databeskyttelsesrevision, jf. artikel 58, stk. 1, litra b, når et kontrolorgan underretter om overtrædelse af kodeksen.

5.23.3.5. Forordningens artikel 41, stk. 5 – Tilbagekaldelse af akkreditering
Af forordningens artikel 41, stk. 5, fremgår det, at den kompetente tilsynsmyndighed tilbagekalder akkrediteringen af et organ som omhandlet i stk. 1, hvis betingelserne for akkreditering ikke er eller ikke længere er opfyldt, eller hvis foranstaltninger truffet af organet overtræder denne forordning.

Et eksempel på, at et organ ikke længere opfylder "betingelserne for akkreditering", kan være, at organet ikke længere kan leve op til de betingelser for akkreditering, der følger af artikel 41, stk. 2, herunder f.eks. hvis organet mister ekspertise eller får opgaver/pligter, der kan føre til en interessekonflikt.

Forordningen ses ikke at specificere, hvordan en tilsynsmyndighed skal blive opmærksom på, at et akkrediteret organ ikke længere lever op til betingelserne for akkreditering. En oplagt måde er naturligvis, at tilsynsmyndigheden med passende intervaller foretager en egentlig kontrol af det akkrediterede organ. Kontrol er dog ikke nødvendigvis den eneste mulighed. F.eks. vil der kunne indgås en aftale mellem tilsynsmyndigheden og det akkrediterede organ om, at organet skal underrette tilsynsmyndigheden, hvis der sker ændringer i organets opgaver, pligter eller ekspertise.

5.23.3.6. Forordningens artikel 41, stk. 6 – Gælder ikke for offentlige myndigheder og organer
Af forordningens artikel 41, stk. 6, fremgår det, at artikel 41 ikke finder anvendelse på behandling, der udføres af offentlige myndigheder og organer, jf. stk. 6. En lignende begrænsning for offentlige myndigheder fremgår ej af artikel 40.

Kontrol af offentlige myndigheders efterlevelse af forordningen skal derimod udføres af tilsynsmyndigheden, efter beføjelserne i artikel 58, hvilket eventuelt kan omfatte behand-

linger, der styres efter en adfærdskodeks. Dette er dog ikke ensbetydende med, at tilsynsmyndigheden forpligtes til at kontrollere, om en adfærdskodeks efterleves eller ej.

5.23.3.7. Bøder til kontrolorganer, der ikke lever op til deres forpligtelser
Det fremgår af forordningens artikel 83, stk. 4, litra c, at overtrædelse af kontrolorganets forpligtelser i henhold til artikel 41, stk. 4, straffes med bøde.

Henset til, hvordan adfærdskodekser kan anvendes af dataansvarlige og databehandlere, er det vigtigt, at et akkrediteret kontrolorgan gør sit arbejde grundigt. Hvis et kontrolorgan ikke gør sit arbejde grundigt, kan dette f.eks. føre til, at organet fejlagtigt kommer til at tilkendegive, at en dataansvarlig eller databehandler overholder forordningen, selvom dette ikke er tilfældet.

5.23.4. Overvejelser
Artikel 41 er en nyskabelse, idet der ikke findes tilsvarende regler i gældende ret. Tilstedeværelsen af akkrediteret organ efter artikel 41 kan ikke anses for at være en forudsætning for anvendelsen af artikel 40, som beskrevet ovenfor om adfærdskodekser.

5.24. Certificering, artikel 42

5.24.1. Præsentation
For at støtte op om den praktiske implementering af forordningen og for at have visse værktøjer, der kan hjælpe dataansvarlige og databehandlere til efterlevelse af forordningen, skal der efter databeskyttelsesforordningens artikel 42 tilskyndes til, at der fastlægges certificeringsmekanismer for databeskyttelse og databeskyttelsesmærkninger og -mærker. Dette skal ske både på nationalt og på EU-plan. Udover ovennævnte hensigtserklæring indeholder artikel 42 også en række krav til certificeringsprocessens indhold.

Bestemmelsen i artikel 42 er ny i forhold til persondataloven og databeskyttelsesdirektivet, idet disse ikke indeholder lignende regler om certificering eller mærkning.

Til trods for, at persondataloven og databeskyttelsesdirektivet ikke indeholder regler om certificering og mærkning, findes der dog allerede i dag enkelte certificerings- og mærkningsordninger, også med forbindelse til EU-medlemsstaternes persondatalovgivning. Som et eksempel herpå kan der henvises til, at det Schleswig-Holstenske datatilsyn i flere år har haft en ordning med databeskyttelsesmærker.[668]

[668] Se mere på det Schleswig-Holstenske datatilsyns hjemmeside.

Begrebet "certificering" kan i daglig tale dække over mange ting, men det handler typisk om at bekræfte bestemte karakteristika, knyttet til f.eks. en organisation, en person, hardware, software, eller andet. Eksempelvis kan certificering af en person handle om, at en person er uddannet til at kunne håndtere en bestemt opgave. Altså en form for eksamensbevis.

Hvordan begrebet "certificering" skal forstås i databeskyttelsesforordningens forstand vil umiddelbart afhænge af de certificeringsmekanismer, der omtales i artikel 42, stk. 1, men som endnu ikke er defineret. Det fremgår dog tydeligt af artikel 42, at bestemmelsen vedrører certificering af behandlingsaktiviteter.

Det må antages, at certificering og mærkning vil få en vis udbredelse med databeskyttelsesforordningen, idet forordningen bl.a. hæfter certificering og mærkning op på helt specifikke krav om behandlingssikkerhed.

5.24.2. Gældende ret

Persondataloven og databeskyttelsesdirektivet indeholder, som nævnt ovenfor, ikke regler om certificering og mærkning.

5.24.3. Forordningen

5.24.3.1. Forordningens artikel 42, stk. 1 – Tilskyndelse til fastlæggelse af certificeringsmekanismer

Det følger af forordningens artikel 42, stk. 1, at medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen navnlig på EU-plan skal tilskynde til fastlæggelse af certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger og -mærker med henblik på at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder denne forordning. Endvidere fremgår det, at mikrovirksomheders og små og mellemstore virksomheders særlige behov skal tages i betragtning.

Med bestemmelsen fastslås det, at det er *behandlingsaktiviteter*, som der kan opnås certificering eller mærkning i forhold til.

I forordningens artikel 4, nr. 2, defineres behandling som enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Når artikel 42, stk. 1, og artikel 4, nr. 2, sammenholdes, må det således modsætningsvist kunne konkluderes, at det ikke er selve det IT-system eller det IT-udstyr, hvori en behandling foregår, der kan opnå certificering eller mærkning, ligesom det heller ikke er organisationer og juridiske personer (dataansvarlig eller databehandler).

Ovennævnte betyder dog ikke, at f.eks. et IT-systems opbygning vil være uden betydning i relation til certificering eller mærkning af behandlingsaktiviteter, idet opbygningen kan have betydning i forhold til forordningens bestemmelser om tekniske og organisatoriske foranstaltninger, jf. artikel 17, 24, 25, 28 og 32.

I IT-systemer og IT-udstyr kan der også foregå flere behandlingsaktiviteter, hvoraf måske kun én af disse aktiviteter er certificeret i henhold til forordningen, mens de andre behandlingsaktiviteter ikke er og måske slet ikke kan blive certificeret. Dette kan f.eks. skyldes, at behandlinger foregår adskilt og på forskellige databeskyttelsesniveauer i samme IT-system. Det kan også gøre en forskel, hvis f.eks. nogle data udelukkende behandles i krypteret form i det specifikke IT-system.

Dataansvarlige og databehandlere, som har opnået certificering eller mærkning af en given behandlingsaktivitet, kan sagtens udføre mange andre behandlingsaktiviteter, der ikke har opnået certificering eller mærkning. Dette kan bl.a. skyldes, at den dataansvarlige eller databehandleren ikke har fundet det formålstjenstligt at opnå certificering eller mærkning af disse øvrige behandlingsaktiviteter. En behandlingsaktivitet, der har opnået certificering eller mærkning, kan til gengæld gå på tværs af flere IT-systemer og organisationer.

Det fremgår af artikel 42, stk. 1, at det er både medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen, der skal tilskynde til fastlæggelse af certificeringsmekanismer og databeskyttelsesmærkninger og -mærker. I forhold til tilsynsmyndighederne og Databeskyttelsesrådet fremgår denne opgave også af henholdsvis forordningens artikel 57, stk. 1, litra n, og artikel 70, stk. 1, litra n.

Når det i artikel 42, stk. 1, fremgår, at tilskyndelsen navnlig skal ske på EU-plan, indebærer dette formentlig, at både tilskyndelsen og fastlæggelsen af certificeringsmekanismer og databeskyttelsesmærkninger og -mærker primært skal ske i et samarbejde på tværs af EU. Dog er ren national tilskyndelse naturligvis ikke udelukket. Når tilskyndelsen navnlig skal ske på EU-plan, kan dette hænge sammen med, at certificering og mærkning må antages at være mest attraktivt for dataansvarlige og databehandlere, hvis en certificering eller et databeskyttelsesmærke er alment kendt på tværs af medlemsstaterne, som f.eks. EU's økologimærke inden for fødevareindustrien. Hvis mange registrerede i EU f.eks. er bekendt med

et bestemt databeskyttelsesmærke, vil det bedre kunne benyttes af dataansvarlige eller databehandlere som et konkurrenceparameter.

Hertil kommer, at "kendte" databeskyttelsesmærker vil kunne være en stor hjælp for de registrerede, når disse hurtigt skal vurdere databeskyttelsesniveauet i forhold til f.eks. et produkt eller en tjenesteydelse, jf. også præambelbetragtning nr. 100. Dette forudsætter imidlertid, at det er nemt for den registrerede at forstå mærkningsordningen, og hvad mærkerne indikerer i forhold til databeskyttelsesniveauet i et produkt eller en tjenesteydelse. En udfordring kan i denne sammenhæng blive at forklare de registrerede, at en certificering eller et databeskyttelsesmærke alene vedrører en behandlingsaktivitet, hvorfor en certificering eller mærkning ikke må opfattes som en garanti for, at al databehandling i relation til et produkt eller en tjenesteydelse nødvendigvis sker i overensstemmelse med forordningen.

Det fremgår af artikel 42, stk. 1, at der skal tages hensyn til mikrovirksomheders og små og mellemstore virksomheders særlige behov. Ligesom det er tilfældet i forhold til adfærdskodekser skyldes dette formentlig, at der er et ønske om at hjælpe små virksomheder – der typisk ikke har en juridisk afdeling eller ressourcerne til at indhente ekstern juridisk rådgivning – til at efterleve forordningens regler ved anvendelse af certificering og mærkning.

I forhold til spørgsmålet om, hvem der skal fastlægge certificeringsmekanismerne henvises der til afsnit 5.25. om certificeringsorganer, artikel 43.

5.24.3.2. Forordningens artikel 42, stk. 2 – Overførsel af oplysninger til tredjelande og internationale organisationer

Af forordningens artikel 42, stk. 2, fremgår det, at certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger eller -mærker, der er godkendt i henhold til artikel 42, stk. 5, ud over overholdelse af de dataansvarlige eller databehandlere, der er omfattet af denne forordning, kan fastlægges med det formål at påvise tilstedeværelse af fornødne garantier afgivet af dataansvarlige eller databehandlere, der i henhold til artikel 3 ikke er omfattet af denne forordning, inden for rammerne af overførsel af personoplysninger til tredjelande eller internationale organisationer, jf. artikel 46, stk. 2, litra f. Det fremgår endvidere, at disse dataansvarlige eller databehandlere, gennem kontrakter eller andre retligt bindende instrumenter, skal afgive bindende tilsagn, som kan håndhæves, om at anvende disse fornødne garantier, herunder for så vidt angår registreredes rettigheder.

5.24.3.3. Forordningens artikel 42, stk. 3 – Certificering som frivillig og gennemsigtig proces

Certificering skal være frivillig og tilgængelig gennem en gennemsigtig proces, jf. stk. 3. Det antages hermed, at en dataansvarlig f.eks. ikke kan påtvinge en databehandler at blive

certificeret, selv om databehandleren skal efterleve forordningen ved en databehandling udført for den dataansvarlige.

At processen skal være gennemsigtig kan betyde, at den skal være nem at forstå og gennemskue. Hvis kravet om gennemsigtighed efterleves, vil det være nemmere for dataansvarlige og databehandlere at vurdere, hvad det indebærer at blive certificeret. Dette kan eventuelt hjælpe dataansvarlige og databehandlere ved deres vurdering af, om det kan betale sig at igangsætte certificeringsprocessen og dermed bruge de ressourcer, det kræver.

5.24.3.4. Forordningens artikel 42, stk. 4 – Ansvar, opgaver og beføjelser ved certificerede behandlinger

Af forordningens artikel 42, stk. 4, fremgår det, at certificering i henhold til artikel 42 ikke indskrænker den dataansvarliges eller databehandlerens ansvar for at overholde denne forordning, og at certificering ikke berører opgaverne og beføjelserne for de tilsynsmyndigheder, der er kompetente i henhold til artikel 55 eller 56.

Ovennævnte må bl.a. betyde, at en dataansvarlig eller en databehandler ikke kan nægte tilsynsmyndigheden at føre tilsyn med eller udstede påbud i forhold til en behandlingsaktivitet, med den begrundelse, at behandlingsaktiviteten er certificeret i henhold til artikel 42.

Herudover vil en dataansvarlig eller en databehandler ikke kunne fralægge sig ansvaret eller en del af ansvaret for overholdelsen af forordningen med den begrundelse, at en behandlingsaktivitet er certificeret i henhold til artikel 42. Dataansvarlige og databehandlere bør således ikke formode, at en behandlingsaktivitet overholder forordningen, udelukkende fordi behandlingsaktiviteten er certificeret.

I forlængelse af ovennævnte må det også antages, at en dataansvarlig eller en databehandler kan ifalde ansvar – og blive pålagt en bøde – hvis den pågældende foretager en behandlingsaktivitet, der ikke er i overensstemmelse med forordningen, selvom aktiviteten er certificeret. Det fremgår dog af forordningens artikel 83, stk. 2, litra j, at overholdelse af godkendte certificeringsmekanismer skal medtages i de hensyn, som tages ved afgørelse om hvorvidt der skal udstedes en administrativ bøde, og størrelsen på den administrative bøde.

5.24.3.5. Forordningens artikel 42, stk. 5 – Udstedelse af certificering

Det fremgår af forordningens artikel 42, stk. 5, at certificering i henhold til artikel 42 skal udstedes af certificeringsorganer, jf. artikel 43, eller af den kompetente tilsynsmyndighed på grundlag af kriterier, der er godkendt af den pågældende kompetente tilsynsmyndighed i henhold til artikel 58, stk. 3, eller af Databeskyttelsesrådet i henhold til artikel 63. Endvide-

re fremgår det, at hvis kriterierne er godkendt af Databeskyttelsesrådet, kan det føre til en fælles certificering, Den Europæiske Databeskyttelsesmærkning.

Certificering kan altså foretages af både certificeringsorganet og tilsynsmyndigheden, mens kriterierne for en certificering kan godkendes af tilsynsmyndigheden eller Databeskyttelsesrådet. Uanset hvem der foretager certificeringen, skal det ske på grundlag af de samme kriterier.

Opgaven med at godkende kriterier for certificering fremgår også af forordningens artikel 57, stk. 1, litra n, der beskriver tilsynsmyndighedens opgaver.

Det fremgår ikke af artikel 42, stk. 5, hvem der skal udarbejde kriterierne for certificering. For mere herom henvises der til 5.25. om certificeringsorganer, artikel 43.

Af artikel 42, stk. 2, fremgår det, at certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger eller -mærker, der er godkendt i henhold til artikel 42, stk. 5, ud over overholdelse af de dataansvarlige eller databehandlere, der er omfattet af denne forordning, kan fastlægges med det formål at påvise tilstedeværelse af fornødne garantier afgivet af dataansvarlige eller databehandlere, der i henhold til artikel 3 ikke er omfattet af denne forordning, inden for rammerne af overførsel af personoplysninger til tredjelande eller internationale organisationer, jf. artikel 46, stk. 2, litra f.

Når der i artikel 42, stk. 2, tales om "Certificeringsmekanismer" og "databeskyttelsesmærkninger", må dette antages at være synonymt med "kriterierne" i artikel 42, stk. 5, da førstnævnte begreber ikke optræder i stk. 5. Denne sammenbinding synes også at fremgå af artikel 43, stk. 6, som bl.a. angiver, at alle certificeringsmekanismer og databeskyttelsesmærkninger skal offentliggøres af Databeskyttelsesrådet.

5.24.3.6. Forordningens artikel 42, stk. 6 – Certificeringsmekanismen
Af forordningens artikel 42, stk. 6, fremgår det, at den dataansvarlige eller den databehandler, der forelægger sin behandling for certificeringsmekanismen, skal give det i artikel 43 omhandlede certificeringsorgan eller eventuelt den kompetente tilsynsmyndighed alle oplysninger og adgang til de behandlingsaktiviteter, der er nødvendige for at gennemføre certificeringsproceduren.

Det er ikke specificeret i artikel 42, stk. 6, hvem der skal have behandlingen forelagt, men blot at det skal forelægges certificeringsmekanismen. Hvis tilsynsmyndigheden bliver forelagt behandlingen, har myndigheden i henhold til artikel 58, stk. 3, litra f, beføjelse til at udstede certificering. Udstedelse af certificering fremgår imidlertid ikke af listen over til-

synsmyndighedens opgaver i forordningens artikel 57, stk. 1. Dette betyder formentlig, at tilsynsmyndigheden, hvis den bliver forelagt en behandling, kan vælge at overdrage opgaven til et akkrediteret organ, der også har beføjelse til at udstede certificering, og som netop er blevet akkrediteret til at udføre denne opgave.

Forordningen bruger udtrykket "Certificeringsmekanismer", uden at angive en definition. Hvis der sammenlignes med andre typer af certificeringer, kan man antage, at det bl.a. handler om etablering af en dokumenteret proces med faste tjeklister, test eller lignende elementer, som der kan "eksamineres i". En "Certificeringsmekanisme" kan endvidere indeholde en indikation af, hvad der skal til for at kunne blive certificeret. Disse antagelser om, hvad "Certificeringsmekanismer" kan omhandle, er baseret på, hvordan man kan blive certificeret i forhold til visse eksisterende standarter.

I artikel 42, stk. 6, anvendes udtrykket imidlertid på en speciel måde. Der står: "... dataansvarlige eller databehandler, der forelægger sin behandling for certificeringsmekanismen...". Her synes udtrykket at inkludere det akkrediterede kontrolorgan eller den tilsynsmyndighed, der gennemfører certificeringen.

5.24.3.7. Forordningens artikel 42, stk. 7 – Tidsbegrænsninger og tilbagetrækning
Det fremgår af forordningens artikel 42, stk. 7, at certificering udstedes til en dataansvarlig eller en databehandler for en periode på højst tre år og kan forlænges på de samme betingelser, så længe de relevante krav stadig er opfyldt. Herudover fremgår det, at certificering trækkes tilbage af certificeringsorganerne, jf. artikel 43, eller i givet fald den kompetente tilsynsmyndighed, hvis kravene til certificering ikke er eller ikke længere er opfyldt.

Med artikel 42, stk. 7, fastsættes der således en øvre grænse for, hvor længe en certificering kan være gyldig, ligesom det fastsættes, at en forlængelse ikke kan ske uden en kontrol og bekræftelse af, at kravene stadig bliver opfyldt.

Endvidere fastsættes det med artikel 42, stk. 7, at en certificering – inden gyldighedsperiodens udløb – kan trækkes tilbage, hvis kravene til certificering ikke længere er opfyldt. At kravene ikke længere er opfyldt vil f.eks. kunne konstateres ved, at tilsynsmyndigheden benytter sine beføjelser efter artikel 58, stk. 1, litra c, til at udføre revision af en certificering. At tilsynsmyndigheden regelmæssigt, når det er relevant, skal gennemgå certificeringer fremgår også af opgavebeskrivelsen i forordningens artikel 57, stk. 1, litra o.

Det fremgår ikke af artikel 57 eller 58, hvad der kan begrunde en gennemgang (eller revision), eller hvor ofte den regelmæssige gennemgang skal finde sted. En gennemgang af en certificering kunne f.eks. indgå som en del af et bredere tilsyn (artikel 57, stk. 1, litra a).

Et eksempel på noget, der formentlig vil få tilsynsmyndigheden til at foretage en gennemgang (revision) af en certificering, kunne være, hvis tilsynsmyndigheden bliver bekendt med, at der er problemer med en certificeret behandlingsaktivitet. Tilsynsmyndigheden kan f.eks. blive bekendt dermed i forbindelse med et brud på persondatasikkerheden.

En sådan gennemgang kan også føre til, at tilsynsmyndigheden finder anledning til at kontrollere, om et eventuelt certificeringsorgan har løst sin opgave på tilfredsstillende vis. Der kan derfor være gode grunde til at foretage en gennemgang af en certificering.

Kontrol af overholdelse af kravene til certificering og af betingelserne for akkreditering vil formentlig være en naturlig del af tilsynsmyndighedens undersøgelse af brud på persondatasikkerheden, ikke mindst fordi overholdelse af en godkendt certificeringsmekanisme f.eks. kan være brugt som et element til at påvise overholdelse af kravene i artikel 32, stk. 1, angående behandlingssikkerhed. Det kan i en sådan situation endvidere være relevant at vurdere, om certificeringsmekanismen eller betingelserne for akkreditering har mangler.

Af artikel 42, stk. 7, fremgår det, at certificering *kan* forlænges på de samme betingelser, så længe de relevante *krav* stadig er opfyldt. Det er således ikke sikkert, at en certificering altid *kan* forlænges på samme betingelser. En ændring af kravene eller betingelserne kan bl.a. være begrundet i, at disse er blevet ændret siden sidste certificering blev gennemført.

Når forordningens artikel 42, stk. 5 og 7, sammenholdes kan det udledes, at både certificering, forlængelse af certificering og tilbagetrækning af certificering kan udføres af enten certificeringsorganerne eller den kompetente tilsynsmyndighed.

Idet udstedelse af certificering (artikel 58, stk. 3, litra f) samt tilbagetrækning af certificering (artikel 58, stk. 2, litra h) er en del af tilsynsmyndighedens beføjelser, må det antages, at tilsynsmyndigheden har pligt til at varetage disse opgaver, hvis der ikke findes et akkrediteret organ. Forlængelse af en certificering fremgår ikke af listen over tilsynsmyndighedens beføjelser (artikel 58), men idet tilsynsmyndigheden kan udstede en certificering, må det antages, at tilsynsmyndigheden også har beføjelse til at forlænge en certificering.

Hverken tilbagetrækning eller forlængelse af en certificering er gjort afhængig af, hvilken part der oprindeligt foretog certificeringen. Det må derfor antages, at både tilsynsmyndigheden og det akkrediterede certificeringsorgan kan tilbagetrække og forlænge alle certificeringer. Det skal i den sammenhæng bemærkes, at certificeringsorganet, der oprindeligt udførte certificeringen, i mellemtiden kan have mistet sin akkreditering, hvorved det er nødvendigt, at opgaven varetages af andre.

5.24.3.8. Forordningens artikel 42, stk. 8 – Offentliggørelse

Det fremgår af forordningens artikel 42, stk. 8, at Databeskyttelsesrådet samler alle certificeringsmekanismer og databeskyttelsesmærkninger og -mærker i et register og gør dem offentligt tilgængelige på passende vis.

5.24.3.9. Samspillet mellem forordningens artikel 42 og andre bestemmelser i forordningen

5.24.3.9.1. Samspillet med artikel 24 – Den dataansvarliges ansvar

Efter forordningens artikel 24, stk. 3, kan overholdelse af godkendte certificeringsmekanismer bruges som et element til at påvise overholdelse af den dataansvarliges forpligtelser i henhold til forordningen.

Dette er umiddelbart en meget generel og bred anvisning af, hvordan en certificeringsmekanisme kan anvendes. Hvilke dele af forordningen, der er dækket, afhænger naturligvis af indholdet i certificeringsmekanismen.

5.24.3.9.2. Samspillet med artikel 25 – Databeskyttelse gennem design og standardindstillinger

Af forordningens artikel 25, stk. 3, fremgår det, at en godkendt certificeringsmekanisme i medfør af artikel 42 kan blive brugt som et element til at påvise overholdelse af kravene i artikel 25 stk. 1 og 2.

Det i den forbindelse er værd at bemærke, at der ikke i artikel 25, stk. 3, henvises til muligheden for at benytte en adfærdskodeks som element til at påvise overholdelse af kravene i artikel 25 stk. 1 og 2. Mulighederne for at benytte adfærdskodeks og certificering er ellers identiske i flere artikler, men altså ikke her. Der er dermed færre muligheder for at påvise overholdelse af kravene om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, end forpligtelser angående f.eks. behandlingssikkerhed i artikel 32.

5.24.3.9.3. Samspillet med artikel 28 – Databehandlers påvisning af fornødne garantier

I henhold til forordningens artikel 28, stk. 5, kan en databehandlers overholdelse af en godkendt certificeringsmekanisme som omhandlet i artikel 42 bruges som et element til at påvise fornødne garantier som omhandlet i artikel 28, stk. 1 og 4.

Dette omfatter databehandleres garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder.

5.24.3.9.4. Samspillet med artikel 32 – Behandlingssikkerhed
Af forordningens artikel 32, stk. 3, fremgår det, at overholdelse af en godkendt certificeringsmekanisme, som omhandlet i artikel 42, kan bruges som et element til at påvise den dataansvarliges og databehandlerens overholdelse af kravene i artikel 32, stk. 1.

5.24.3.9.5. Samspillet med artikel 46 – Overførsler omfattet af fornødne garantier
Det fremgår af forordningens artikel 46, stk. 2, litra f, at de fornødne garantier i forbindelse med overførsel af personoplysninger til et såkaldt usikkert tredjeland – uden krav om specifik godkendelse fra en tilsynsmyndighed – kan sikres gennem en godkendt certificeringsmekanisme i medfør af artikel 42 sammen med bindende tilsagn, som kan håndhæves, fra den dataansvarlige eller databehandleren i tredjelandet om at anvende de fornødne garantier, herunder vedrørende registreredes rettigheder.

5.24.3.9.6. Samspillet med artikel 83 – Administrative bøder
Af forordningens artikel 83, stk. 2, litra j, fremgår det, at der ved afgørelsen af, hvorvidt der skal pålægges en administrativ bøde, og om den administrative bødes størrelse i hver enkelt sag, skal tages behørigt hensyn til, om godkendte certificeringsmekanismer er overholdt.

Overholdelse af en godkendt certificeringsmekanisme i forbindelse med en given behandling vil således f.eks. kunne inddrages som en formildende omstændighed ved fastsættelsen af en eventuel bødes størrelse.

Det er i den forbindelse vigtigt at være opmærksom på, at overholdelse af en certificeringsmekanisme ikke i sig selv er bevis på overholdelse af forordningen, heller ikke for så vidt angår specifikke artikler i forordningen. Overholdelse af en certificeringsmekanisme kan dermed ikke fritage en dataansvarlig eller databehandler for ansvar, hvorfor det heller ikke kan antages, at en bøde helt kan frafaldes alene med baggrund i overholdelse af en godkendt certificeringsmekanisme.

5.24.4. Overvejelser
Artikel 42 er en nyskabelse, idet der ikke findes tilsvarende regler i gældende dansk ret.

Der mangler endnu at blive fastlagt en del elementer, før det eventuelt bliver tydeligt for dataansvarlige og databehandlere, hvilke behandlingsaktiviteter det kan betale sig at få certificeret.

Da certificering nævnes i flere artikler om behandlingssikkerhed, og den potentielt positive effekt det kan have på administrative bøder, har certificering potentiale til at få en stor betydning under forordningen.

Noget taler endvidere for, at der bør etableres et samarbejde på tværs af EU, f.eks. omkring tilskyndelse til fastsættelse af certificeringsmekanismer.

5.25. Certificeringsorganer, artikel 43

5.25.1. Præsentation

Efter databeskyttelsesforordningens artikel 42 skal medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen tilskynde navnlig på EU-plan til fastlæggelse af certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger og -mærker med henblik på at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder forordningen. Mikrovirksomheders og små og mellemstore virksomheders særlige behov skal i den forbindelse tages i betragtning.

Certificeringsmekanismer i henhold til 42 vil således kunne benyttes af dataansvarlige og databehandlere til at påvise, at deres behandlingsaktiviteter overholder forordningen.

Når certificeringsmekanismer skal kunne benyttes af dataansvarlige og databehandlere til at påvise, at deres behandlingsaktiviteter overholder forordningen, er der samtidig et behov for, at der føres kontrol med, om godkendte certificeringsmekanismer overholdes i praksis. I forordningens artikel 43 fastsættes der nærmere regler for kontrol med godkendte certificeringsmekanismer. Disse regler gennemgås i det følgende.

5.25.2. Gældende ret

Der findes ingen regler om kontrol af godkendte certificeringsmekanismer i hverken databeskyttelsesdirektivet eller persondataloven.

5.25.3. Databeskyttelsesforordningen

5.25.3.1. Forordningens artikel 43, stk. 1 – Certificeringsorganers akkreditering og beføjelser

Af forordningens artikel 43, stk. 1, fremgår det, at certificeringsorganer, der har et passende ekspertiseniveau for så vidt angår databeskyttelse, udsteder og forlænger certificering, efter at have underrettet tilsynsmyndigheden for at gøre det muligt for den at udøve sine beføjelser i henhold til artikel 58, stk. 2, litra h), hvis det er nødvendigt, uden at dette berører den kompetente tilsynsmyndigheds opgaver og beføjelser i henhold til artikel 57 og 58.

Det fremgår endvidere af bestemmelsen, at medlemsstaterne sikrer, at disse certificeringsorganer akkrediteres af en eller begge af følgende:

a) den tilsynsmyndighed, der er kompetent i henhold til artikel 55 eller 56

b) det nationale akkrediteringsorgan, som er udpeget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008[669] i overensstemmelse med EN-ISO/IEC 17065/2012 og med de supplerende krav, der er fastsat af den tilsynsmyndighed, som er kompetent i henhold til artikel 55 eller 56.

Certificering sker således efter, at certificeringsorganet har underrettet tilsynsmyndigheden, så denne har haft mulighed for at udøve sine beføjelser i henhold til artikel 58, stk. 2, litra h, hvilket blandt andet omfatter muligheden for at give påbud om ikke at udstede en certificering.

Når overladelse af kontrollen med overholdelsen af en certificeringsmekanisme ikke berører den kompetente tilsynsmyndigheds opgaver og beføjelser, betyder dette bl.a., at tilsynsmyndigheden stadig har sine opgaver og beføjelser for så vidt angår behandlingsaktiviteter, der foregår i tilknytning til en certificeringsmekanisme, som kontrolleres af et akkrediteret organ. Tilsynsmyndigheden kan dermed fortsat føre tilsyn med behandlingsaktiviteter, både generelt og i forhold til eventuelle specifikke områder, som måtte være omfattet af certificeringsmekanismer.

I forhold til akkreditering af et certificeringsorgan, fremgår det, at dette kan udføres af den kompetente tilsynsmyndighed eller af et nationalt akkrediteringsorgan. Når akkreditering udføres af sidstnævnte, er det vigtigt at være opmærksom på, at den kompetente tilsynsmyndighed kan stille supplerende krav.

Tilsynsmyndighedens beføjelser til akkreditering af certificeringsorganer fremgår af artikel 58, stk. 3, litra e.

5.25.3.2. Forordningens artikel 43, stk. 2 – Krav til certificeringsorganer

Det fremgår af forordningens artikel 43, stk. 2, at certificeringsorganer, som omhandlet i stk. 1, kun akkrediteres i overensstemmelse med artikel 43, stk. 1, hvis de har:

[669] Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af Rådets forordning (EØF) nr. 339/93 (EUT L 218 af 13.8.2008, s. 30).

a) påvist deres uafhængighed og ekspertise med hensyn til certificeringens genstand til den kompetente tilsynsmyndigheds tilfredshed

b) påtaget sig at opfylde kriterierne i artikel 42, stk. 5, og er blevet godkendt af den tilsynsmyndighed, der er kompetent i henhold til artikel 55 eller 56, eller af Databeskyttelsesrådet i henhold til artikel 63

c) fastlagt procedurer for udstedelse, regelmæssig revision og tilbagetrækning af databeskyttelsescertificeringer, -mærkninger og -mærker

d) fastlagt procedurer og ordninger for behandling af klager over overtrædelser af certificering eller den måde, hvorpå certificering er blevet eller bliver gennemført af en dataansvarlig eller en databehandler, og for, hvordan disse procedurer og ordninger gøres gennemsigtige for registrerede og offentligheden, og

e) vist til den kompetente tilsynsmyndigheds tilfredshed, at deres opgaver og pligter ikke fører til en interessekonflikt.

I artikel 43, stk. 2, præciseres det bl.a., at et certificeringsorgan ikke alene skal have ekspertise inden for databeskyttelse og certificering generelt, men at organet også skal have ekspertise for så vidt angår certificeringens genstand, altså det som certificeringen specifikt retter sig mod. Der må således kunne stilles ret høje krav til et certificeringsorgan.

Kravene i stk. 2 gælder i øvrigt uanset, om en akkreditering foretages af den kompetente tilsynsmyndighed eller et nationalt akkrediteringsorgan. Et nationalt akkrediteringsorgan vil derfor også skulle sikre sig, at kravene i stk. 2, litra a og e, er påvist til den kompetente tilsynsmyndigheds tilfredshed.

Efter artikel 43, stk. 2, litra b, kræver akkreditering endvidere, at certificeringsorganet påtager sig at opfylde kriterierne i artikel 42, stk. 5, og er blevet godkendt af tilsynsmyndigheden eller Databeskyttelsesrådet.

I artikel 43, stk. 2, litra c og d, stilles der krav til certificeringsorganets procedurer og ordninger for udstedelse, regelmæssig revision og tilbagetrækning af databeskyttelsescertificeringer, -mærkninger og -mærker, behandling af klager over overtrædelser af certificering eller gennemførelse af certificering, samt hvordan disse procedurer og ordninger gøres gennemsigtige for registrerede og offentligheden. Før en akkreditering kan finde sted, skal certificeringsorganet altså have dokumenteret, hvorledes det fremadrettet vil udføre sine opgaver i rollen som certificeringsorgan.

Når det specifikt fremgår af artikel 43, stk. 2, litra d, at de procedurer mv., som et certificeringsorgan skal have for bl.a. behandling af klagesager, skal være gennemsigtige, må dette antages at indebære, at procedurerne skal være forståelige for de registrerede og offentligheden i almindelighed. Hvis procedurerne ikke er forståelige for de registrerede og offentligheden, vil hele formålet med en certificeringsordning gå tabt, idet en sådan netop er tiltænkt at skulle hjælpe de registrerede til hurtigt at kunne vurdere databeskyttelsesniveauet i forhold til relevante produkter og tjenesteydelser, jf. også præambelbetragtning nr. 100.

5.25.3.3. Forordningens artikel 43, stk. 3 – Kriterier for akkreditering

Af forordningens artikel 43, stk. 3, fremgår det, at akkreditering af de i artikel 43, stk. 1 og 2, omhandlede certificeringsorganer finder sted på grundlag af kriterier, der er godkendt af den tilsynsmyndighed, som er kompetent i henhold til artikel 55 eller 56, eller af Databeskyttelsesrådet i henhold til artikel 63. Det fremgår endvidere, at disse krav – i tilfælde af akkreditering i henhold til nærværende artikels stk. 1, litra b) – supplerer kravene i forordning (EF) nr. 765/2008 og de tekniske regler, der beskriver certificeringsorganers metoder og procedurer.

I relation til ovennævnte fremgår det af artikel 70, stk. 1, litra p, at Databeskyttelsesrådet har til opgave at angive de krav, der er omhandlet i artikel 43, stk. 3, med henblik på akkreditering af certificeringsorganer i henhold til artikel 42. Endvidere fremgår det af artikel 57, stk. 1, litra p, at tilsynsmyndigheden har til opgave at opstille og offentliggøre kriterierne for akkreditering af et certificeringsorgan i henhold til artikel 43.

5.25.3.4. Forordningens artikel 43, stk. 4 – Tidsbegrænsning for akkreditering og certificeringsorganets ansvar

Det fremgår af forordningens artikel 43, stk. 4, at de i stk. 1 omhandlede certificeringsorganer er ansvarlige for en korrekt vurdering, der fører til certificering eller tilbagetrækning af certificering, uden at dette berører den dataansvarliges eller databehandlerens ansvar for at overholde denne forordning. Herudover fremgår det, at akkreditering udstedes for en periode på højst fem år og kan forlænges på samme betingelser, såfremt certificeringsorganet opfylder de i denne artikel fastsatte krav.

Med artikel 43, stk. 4, bliver det fastslået, at et certificeringsorgan er ansvarlig for, at det er en korrekt vurdering, der fører til certificering eller tilbagetrækning af certificering. Dette må antages at hænge sammen med, at overtrædelse af certificeringsorganets forpligtelser i henhold til denne artikel og specifikt stk. 4, kan straffes med bøde, jf. artikel 83, stk. 4, litra b.

Det er også vigtigt at være opmærksom på, at det fremhæves, at det at en behandlingsaktivitet er blevet certificeret, ikke ændrer på de dataansvarlige og databehandlernes ansvar i forhold til efterlevelse af forordningen.

5.25.3.5. Forordningens artikel 43, stk. 5 – Oplysninger til tilsynsmyndigheden
Af forordningens artikel 43, stk. 5, fremgår det, at de i stk. 1 omhandlede certificeringsorganer giver de kompetente tilsynsmyndigheder oplysninger om begrundelsen for at udstede eller tilbagetrække den certificering, der er anmodet om.

Når det tages i betragtning, at en udstedelse eller en tilbagetrækning af en certificering følger konkrete krav, og sker efter fastlagte procedurer for certificeringsorganets udførsel af sine opgaver, må det kunne forventes, at certificeringsorganet kan udforme en rimelig præcis og konkret beskrivelse af, hvad der har ført til udstedelse eller tilbagetrækning af en certificering.

5.25.3.6. Forordningens artikel 43, stk. 6 – Offentliggørelsen af kriterier, certificeringsmekanismer og databeskyttelsesmærkninger
Det fremgår af forordningens artikel 43, stk. 6, at tilsynsmyndigheden offentliggør de i artikel 43, stk. 3, omhandlede krav og de i artikel 42, stk. 5, omhandlede kriterier i lettilgængelig form. Det fremgår tillige, at tilsynsmyndighederne meddeler disse krav og kriterier til Databeskyttelsesrådet. Endelig fremgår det, at Databeskyttelsesrådet samler alle certificeringsmekanismer og databeskyttelsesmærkninger i et register og gør dem offentligt tilgængelige på passende vis.

Når der i nærværende bestemmelse henvises til "kravene" i stk. 3, må dette betyde de "kriterier", som er omtalt i stk. 3 − kriterier der er enten er godkendt af den kompetente tilsynsmyndighed eller af Databeskyttelsesrådet.

Brugen af udtrykket "kriterier" i artikel 43, stk. 6, 3. punktum, synes at relatere sig til begreberne "certificeringsmekanismer og databeskyttelsesmærkninger", der skal offentliggøres i et samlet register. Denne relation mellem "kriterier" og "certificeringsmekanismer og databeskyttelsesmærkninger", ses også ved at sammenholde artikel 42, stk. 2 og 5.

Det fremgår af artikel 70, stk. 1, litra p, om Databeskyttelsesrådets opgaver, at rådet bl.a. har til opgave at føre et offentligt register over akkrediterede organer i henhold til artikel 43, stk. 6.

5.25.3.7. Forordningens artikel 43, stk. 7 – Tilbagekaldelse af akkreditering
Af forordningens artikel 43, stk. 7, fremgår det, at hvis betingelserne for en akkreditering ikke er eller ikke længere er opfyldt, eller hvis de foranstaltninger, som organet har truffet, overtræder denne forordning, tilbagekalder den kompetente tilsynsmyndighed eller det nationale akkrediteringsorgan en akkreditering af et certificeringsorgan, jf. artikel 43, stk. 1, uden at dette berører kapitel VIII.

Efter artikel 43, stk. 7, kan tilbagekaldelse af akkreditering således ske ved begge de parter, der kan akkreditere. Det er i den forbindelse uden betydning, hvem der oprindeligt stod for akkrediteringen.

Et eksempel på en situation, hvor en tilsynsmyndighed formentlig vil foretage en kontrol af, om et certificeringsorganet har løst sin opgave på tilfredsstillende vis, kan være, hvis tilsynsmyndigheden bliver bekendt med, at der er problemer med en certificeret behandlingsaktivitet. Tilsynsmyndigheden kan f.eks. blive bekendt med dette i forbindelse med et brud på persondatasikkerheden.

For så vidt angår Databeskyttelsesrådet fremgår det af artikel 70, stk. 1, litra p, at rådet også har til opgave at foretage akkreditering af certificeringsorganer og foretage regelmæssig revision heraf i henhold til artikel 43. "Revision" af en akkreditering indikerer, at der i løbet af perioden for et organs akkreditering (på højst 5 år), kan ske kontrol af, om kravene stadig er opfyldt, idet der i afkræftende fald kan ske en tilbagetrækning af akkrediteringen. For Databeskyttelesrådets vedkommende er der tilsyneladende tale om en *regelmæssig* revision, hvorfor rådet ikke behøver en konkret anledning til at indlede en sådan, herunder f.eks. som følge af et brud på persondatasikkerheden.

I artikel 43, stk. stk. 7, omtales "foranstaltninger" truffet af organet, og at disse "foranstaltninger" kan overtræde forordningen. Det er ikke nærmere defineret, hvad disse foranstaltninger kan gå ud på, men der kan måske være tale om de handlinger, som certificeringsorganet udfører, f.eks. angående høring af parter. Udføres en krævet høring f.eks. ikke, kan dette således måske føre til, at en akkreditering tilbagekaldes.

5.25.3.8. Forordningens artikel 43, stk. 8 – Kommissionens beføjelser angående certificeringsmekanismer
Det fremgår af artikel 43, stk. 8, at Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 92 med henblik på at fastlægge de krav, der skal tages i betragtning vedrørende de certificeringsmekanismer for databeskyttelse, der er omhandlet i artikel 42, stk. 1.

Præambelbetragtning nr. 166 understøtter dette og uddyber, at retsakter også bør dække mærkningen. Betragtning nr. 166 angiver, at der navnlig bør vedtages delegerede retsakter om kriterier for og krav til certificeringsmekanismer, oplysninger, der skal fremgå af standardiserede ikoner, og procedurer for tilvejebringelse af sådanne ikoner.

Det må forventes, at EU-Kommissionen vil specificere indholdet i certificeringsmekanismer via delegerede retsakter. Dette udelukker dog ikke, at nationale tilsynsmyndigheder kan fastsætte kriterier for certificeringsmekanismer, der skal gælde nationalt. Sådanne nationale kriterier kan godkendes af Databeskyttelsesrådet, hvorved anvendelsesområdet må forventes at blive udvidet til EU.

5.25.3.9. Forordningens artikel 43, stk. 9 – Kommissionens beføjelser angående tekniske standarder for certificeringsmekanismer
Det fremgår af artikel 43, stk. 9, at Kommissionen kan vedtage gennemførelsesretsakter, der fastlægger tekniske standarder for certificeringsmekanismer og databeskyttelsesmærkninger og -mærker samt ordninger, der har til formål at fremme og anerkende disse certificeringsmekanismer, mærkninger og -mærker. Endvidere fremgår det, at disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 92, stk. 2.

5.25.3.10. Særligt om forholdet mellem artikel 43 og forordningens bødebestemmelser
5.25.3.10.1. Bøder til dataansvarlige og databehandlere, der ikke lever op til deres forpligtelser
Det fremgår af artikel 83, stk. 4, litra a, at dataansvarlige og databehandleres overtrædelse af deres forpligtelser i henhold til artikel 42 og 43, kan straffes med bøde.

Overholdelse af både en godkendt certificeringsmekanisme og en godkendt adfærdskodeks kan bruges af dataansvarlige og databehandlere til at underbygge, at en behandling sker i overensstemmelse med forordningen, jf. artikel 83, stk. 2, litra j.

5.25.3.10.2. Bøder til kontrolorganer, der ikke lever op til deres forpligtelser
Af forordningens artikel 83, stk. 4, litra c, fremgår det, at overtrædelse af certificeringsorganets forpligtelser i henhold til artikel 41, stk. 4, kan straffes med bøde.

Henset til, hvordan overholdelse af certificeringsmekanismer kan anvendes af dataansvarlige og databehandlere, er det vigtigt, at et akkrediteret kontrolorgan gør sit arbejde grundigt. Hvis et kontrolorgan ikke gør sit arbejde grundigt, kan dette f.eks. føre til, at organet fejlagtigt kommer til at tilkendegive, at en dataansvarlig eller en databehandler overholder forordningen, selvom dette ikke er tilfældet.

5.25.4. Overvejelser

Både certificering og akkreditering af certificeringsorganer er nyskabelser, idet der ikke findes tilsvarende regler i gældende ret.

Da certificering nævnes i flere artikler om behandlingssikkerhed og den potentiel positive effekt det kan have på administrative bøder, har certificering i henhold til artikel 42 potentiale til at få stor betydning fremover.