JUSTITSMINISTERIET

Databeskyttelsesforordningen

– og de retlige rammer for dansk lovgivning

Betænkning nr. 1565

Del I – bind 2

Betænkning om

Databeskyttelsesforordningen (2016/679)

– og de retlige rammer for dansk lovgivning

Del I, bind 2

Betænkning nr. 1565

Indholdsfortegnelse

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

1. Indledning 9

2. Forordningens kapitel I: Generelle bestemmelser 21

2.1. Anvendelsesområde, artikel 2 og 3 21

2.2. Rent privat karakter 39

2.3. Definitioner, artikel 4 43

2.4. Det danske registerbegreb 74

3. Forordningens kapitel II: Principper 81

3.1. Principper for behandling af personoplysninger, artikel 5 og artikel 6, stk. 4 81

3.2. Forskning og statistik, artikel 5, stk. 1, litra b 102

3.3. Lovlig behandling af ikke-følsomme oplysninger, artikel 6, stk. 1 113

3.4. Lovlig behandling af ikke-følsomme oplysninger – nationalt råderum, artikel 6, stk. 2-3 141

3.5. Betingelser for samtykke, artikel 7 170

3.6. Børns samtykke i forbindelse med informationssamfundstjenester, artikel 8 185

3.7. Følsomme oplysninger, artikel 9, stk. 1 189

3.8. Hjemler til behandling af følsomme oplysninger, artikel 9, stk. 2-3 194

3.9. Medlemsstaternes råderum (ved behandling af følsomme oplysninger), artikel 9, stk. 4 231

3.10. Strafbare forhold, herunder straffe- og børneattester, artikel 10, 1. pkt. 233

3.11. Register over straffedomme, artikel 10, 2. pkt. 248

3.12. Behandling, der ikke kræver identifikation, artikel 11 252

3.13. Retsinformation 256

4. Forordningens kapitel III: Den registreredes rettigheder 262

4.1. Gennemsigtig oplysning, artikel 12 262

4.2. Processuelle spørgsmål om registreredes rettigheder, artikel 12, stk. 3-8 265

4.3. Oplysningspligt ved indsamling hos den registrerede, artikel 13 279

4.4. Oplysningspligt, hvis personoplysningerne ikke er indsamlet hos den registrerede, artikel 14 296

4.5. Indsigtsretten, artikel 15 312

4.6. Berigtigelse, artikel 16 325

4.7. Ret til sletning (”retten til at blive glemt”), artikel 17 330

4.8. Ret til begrænsning af behandling, artikel 18 338

4.9. Underretningspligt, artikel 19 342

4.10. Retten til dataportabilitet, artikel 20 346

4.11. Ret til indsigelse, artikel 21 355

4.12. Automatiske afgørelser, artikel 22 370

4.13. Begrænsninger af rettighederne, artikel 23 389

5. Forordningens kapitel IV: Dataansvarlig og databehandler 405

5.1. Den dataansvarliges ansvar, artikel 24 405

5.2. Databeskyttelse gennem design og standardindstillinger, artikel 25 410

5.3. Fælles dataansvar, artikel 26 423

5.4. Repræsentanter, artikel 27 426

5.5. Databehandler, artikel 28 429

5.6. Instruks, artikel 29 442

5.7. Fortegnelser over behandlingsaktiviteter, artikel 30, stk. 1-4 443

5.8. Fortegnelser over behandlingsaktiviteter – undtagelsen i artikel 30, stk. 5 464

5.9. Samarbejde med tilsynsmyndigheden, artikel 31 467

5.10. Behandlingssikkerhed, artikel 32 469

5.11. Anmeldelse af brud på sikkerheden, artikel 33 490

5.12. Underretning om sikkerhedsbrud til den registrerede, artikel 34 506

5.13. Konsekvensanalyser vedrørende databeskyttelse, artikel 35 522

5.14. Høring af tilsynsmyndigheden, artikel 36 537

5.15. Krigsreglen 544

5.16. Cloud computing 551

5.17. Privates forpligtelse til at udpege en databeskyttelsesrådgiver, artikel 37 561

5.18. Offentlige myndigheder og organers forpligtelse til at udpege en databeskyttelsesrådgiver, artikel 37 569

5.19. Artikel 37, stk. 4, bl.a. om muligheden for danske særregler 573

5.20. Databeskyttelsesrådgiverens stilling og kvalifikationer, artikel 37, stk. 5-6, og artikel 38 574

5.21. Databeskyttelsesrådgiverens opgaver, artikel 39 og 35, stk. 2 585

5.22. Adfærdskodekser, artikel 40 588

5.23. Kontrol af godkendte adfærdskodekser, artikel 41 606

5.24. Certificering, artikel 42 612

5.25. Certificeringsorganer, artikel 43 622

6. Forordningens kapitel V: Overførsler af personoplysninger til tredjelande eller internationale organisationer 630

6.1. Generelt princip for overførsler, artikel 44 630

6.2. Overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, artikel 45 638

6.3. Overførsler omfattet af fornødne garantier, artikel 46 657

6.4. Bindende virksomhedsregler, artikel 47 670

6.5. Overførsel uden hjemmel i EU-retten, artikel 48 712

6.6. Undtagelser i særlige situationer, artikel 49 717

6.7. Internationalt samarbejde om beskyttelse af personoplysninger, artikel 50 734

7. Forordningens kapitel VI: Uafhængige tilsynsmyndigheder 739

7.1. Tilsynsmyndighed, artikel 51, 53 og 54 739

7.2. Uafhængighed, artikel 52 748

7.3. Regler om oprettelse af en tilsynsmyndighed, artikel 54 766

7.4. Tilsynsmyndighedens kompetence, artikel 55 og 56 769

7.5. Tilsynsmyndighedens opgaver, artikel 57 773

7.6. Åbenbart grundløse eller uforholdsmæssige anmodninger, artikel 57, stk. 4 783

7.7. Tilsynsmyndighedens beføjelser, artikel 58 788
7.8. Adgang til oplysninger og lokaler, artikel 58, stk. 1, litra e og f..... 807
7.9. Aktivitetsrapport, artikel 59..... 811

8. Forordningens kapitel VII: Samarbejde og sammenhæng 814
8.1. Samarbejde mellem tilsynsmyndigheder, artikel 60..... 814
8.2. Gensidig bistand og fælles aktiviteter, artikel 61 og 62 821
8.3. Sammenhæng, artikel 63-67 832
8.4. Databeskyttelsesrådet, artikel 68 og artikel 70-76..... 847
8.5. Databeskyttelsesrådets uafhængighed, artikel 69 859

9. Forordningens kapitel VIII: Retsmidler, ansvar og sanktioner 862
9.1. Ret til at indgive klage, artikel 77 862
9.2. Adgang til effektive retsmidler over for en tilsynsmyndighed, artikel 78..... 869
9.3. Effektive retsmidler over for en dataansvarlig eller databehandler, artikel 79 .. 878
9.4. Repræsentation af den registrerede, artikel 80 883
9.5. Udsættelse af en sag, artikel 81 891
9.6. Ret til erstatning og erstatningsansvar, artikel 82 898
9.7. Generelle betingelser for pålæggelse af administrative bøder, artikel 83, stk. 1–6 918
9.8. Bøder til offentlige myndigheder, artikel 83, stk. 7 927
9.9. Proceduremæssige garantier, artikel 83, stk. 8 930
9.10. Administrative bøder i Danmark, artikel 83, stk. 9 932
9.11. Sanktioner, artikel 84..... 938

10. Forordningens kapitel IX: Bestemmelser vedrørende specifikke behandlingssituationer 948
10.1. Rammerne i artikel 85 vedrørende ytrings- og informationsfrihed..... 948
10.2. Rammerne i artikel 86 om behandling og aktindsigt i officielle dokumenter mv. 959
10.3. Rammerne i artikel 87 vedrørende nationalt identifikationsnummer..... 966

10.4. Rammerne i artikel 88 vedrørende behandling i forbindelse med ansættelsesforhold 970

10.5. Rammerne i artikel 89, stk. 1 og 2 samt 4, vedrørende videnskabelige og historiske forskningsformål og statistiske formål..... 981

10.6. Rammerne i artikel 89, stk. 1 og 3 samt 4, vedrørende arkivformål i samfundets interesse 990

10.7. Rammerne i artikel 90 for nationale regler om tilsynsmyndighedernes adgang til oplysninger, som er underlagt tavshedspligt 995

10.8. Rammerne i artikel 91 vedrørende kirkers og religiøse sammenslutningers eksisterende databeskyttelsesregler 998

11. Forordningens kapitel X og XI: Delegerede retsakter, gennemførelsesbestemmelser og afsluttende bestemmelser 1000

11.1. Forordningens kapitel X og XI om afsluttende bestemmelser (artikel 92-99) .. 1000

12. Databeskyttelsesforordningen – forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger 1005

6. Forordningens kapitel V: Overførsler af personoplysninger til tredjelande eller internationale organisationer

6.1. Generelt princip for overførsler, artikel 44

6.1.1. Præsentation

Med databeskyttelsesforordningens artikel 44 fastsættes der et generelt princip for overførsel af personoplysninger til tredjelande eller internationale organisationer.

Det er nyt, at der bliver fastsat et generelt princip, for overførsel af personoplysninger til tredjelande eller internationale organisationer, i en særskilt bestemmelse, men indholdet af princippet i forordningens artikel 44 er umiddelbart kendt fra både persondataloven og databeskyttelsesdirektivet.

6.1.2. Gældende ret

6.1.2.1. Begrebet "tredjeland"

I persondatalovens § 3, nr. 9, defineres et *tredjeland* som en stat, som ikke indgår i det Europæiske Fællesskab (EU), og som ikke har gennemført aftaler, der er indgået med EU, og som indeholder regler svarende til databeskyttelsesdirektivet (de såkaldte EØS-lande).[670]

Alle andre lande end EU-lande og EØS-lande er således at betragte som tredjelande i persondatalovens forstand.

6.1.2.2. Begrebet "overførsel"

Der er i persondatalovens § 27 fastsat nærmere regler for, hvornår der må *overføres* personoplysninger til et tredjeland.

Persondatalovens § 27 har sin baggrund i databeskyttelsesdirektivets artikel 25 og 26, hvor der dog i stedet for *overførsel* anvendes udtrykket *videregivelse* af personoplysninger til tredjelande.

Diskrepansen mellem ordlyden i henholdsvis persondataloven og databeskyttelsesdirektivet er nærmere beskrevet i Registerudvalgets betænkning nr. 1345. På side 283-284 i betænkningen fremgår det således bl.a., at reglerne om *overførsel* af oplysninger til tredjelande er indeholdt i databeskyttelsesdirektivets artikel 25 og 26. Det fremgår endvidere af betænkning nr. 1345, at et særligt spørgsmål, som udvalget har overvejet, er betydningen

[670] Ifølge EØS-Kommiteens beslutning 83/99 af 25. juni 1999 er EØS-landene Island, Liechtenstein og Norge forpligtet til at implementere databeskyttelsesdirektivet.

af, at der i disse bestemmelser samt i overskriften til direktivets kapitel 4 er anvendt udtrykket *"videregivelse"*. Det bemærkes herved i betænkningen, at udtrykket "videregivelse" i den gældende registerlovgivning benyttes om en overførsel af oplysninger til enhver anden end den registrerede, den dataansvarlige, databehandleren og personer under den dataansvarlige eller databehandlerens direkte myndighed. Det fremgår endvidere af betænkningen, at en overførsel af oplysninger til en databehandler eller personer under databehandlerens direkte myndighed betegnes som en "overladelse" af oplysningerne og altså ikke som en videregivelse. Når personer under den dataansvarliges direkte myndighed anvender oplysningerne, betegnes det som "intern anvendelse" af oplysningerne og altså heller ikke som en videregivelse.

Det fremgår endvidere af betænkning nr. 1345, at det forhold, at der i bestemmelserne i artikel 25 og 26 samt i overskriften til direktivets kapitel 4 tales om "videregivelse" efter udvalgets opfattelse ikke kan antages at føre til, at disse regler alene omfatter overførsel af oplysninger til enhver anden end den registrerede, den dataansvarlige, databehandleren og personer under den dataansvarlige eller databehandlerens direkte myndighed. Reglerne må med andre ord, ifølge Registerudvalget, antages at have et bredere sigte. Der lægges herved vægt på i betænkningen, at der i den engelske version af direktivet er benyttet udtrykket "transfer", og at der i den franske udgave af direktivet tales om "transfert". Hertil kommer, at der i den tyske udgave af direktivet er anvendt udtrykket "Übermittlung", hvilket betyder oversendelse, transmission eller lignende. Registerudvalget tillægger det endvidere betydning, at overførsel af oplysninger til personer, der under den dataansvarliges direkte myndighed er beføjet til at behandle oplysningerne ("intern anvendelse"), ligesom anden form for overførsel kan indebære en risiko for krænkelse af den registreredes integritet (rettigheder og frihedsrettigheder). Det antages derfor i betænkningen, at også sådan overførsel af oplysninger er omfattet af reguleringen i direktivets artikel 25 og 26. Det bemærkes i den forbindelse i betænkningen, at det forhold, at en person, som er underlagt den dataansvarliges instruktionsbeføjelse, ikke må behandle oplysningerne i strid med den dataansvarliges instruktioner, ikke kan antages at ændre herved. Tilsvarende må antages at gælde for så vidt angår en databehandler i et tredjeland.

På den anførte baggrund fandt Regiserudvalget, at bestemmelserne i direktivets artikel 25 og 26 må antages at omfatte enhver form for overførsel af oplysninger til tredjelande, uanset om der er tale om en videregivelse i den betydning, hvori dette begreb benyttes i dag, eller en overladelse (det være sig ekstern eller intern). I det udarbejdede lovudkast i betænkningen er udtrykket "overførsel" derfor anvendt som en samlebetegnelse for henholdsvis videregivelse og overladelse/intern anvendelse.

6.1.2.3. Praksis i forhold til begrebet "overførsel"

EU-Domstolen og Datatilsynet har i to sager nærmere behandlet rækkevidden af begrebet *overførsel* af personoplysninger til et tredjeland.

6.1.2.3.1. I sag C-101/01, Lindqvist, har EU-Domstolen i en præjudiciel afgørelse[671] bl.a. taget stilling til, om der er tale om en overførsel af personoplysninger til et tredjeland, når en EU-borger, ved hjælp af en computer, lægger personoplysninger ud på en hjemmeside, som er lagret på en server i det pågældende EU-land.

EU-Domstolen konkluderer i dommens præmis 71, at der ikke foreligger en overførsel af personoplysninger til et tredjeland i den forstand, hvori udtrykket er anvendt i artikel 25 i databeskyttelsesdirektivet, når en person, der befinder sig i en medlemsstat, lægger personoplysninger ud på en hjemmeside, der er lagret hos vedkommendes udbyder af webhoteltjenester, som er etableret i den samme medlemsstat eller i en anden medlemsstat, hvorved personoplysningerne bliver tilgængelige for alle, der kobler sig på internettet, herunder personer i et tredjeland.

Som begrundelse for sin konklusion henviser EU-Domstolen navnlig til, at det på baggrund af internettets udviklingstrin, på tidspunktet for udarbejdelsen af direktivet, og de manglende kriterier i direktivet for anvendelse af internettet ikke kan formodes, at fællesskabslovgiver har tilsigtet, at begrebet "videregivelse til et tredjeland af personoplysninger" skal omfatte udlæggelse af oplysninger på en hjemmeside, selv om oplysningerne herved gøres tilgængelige i tredjelande. Domstolen henviser endvidere til de praktiske vanskeligheder, som en anden fortolkning af artikel 25 ville føre til (man ville reelt ikke kunne benytte internettet).[672]

Det er i forhold til præmis 71 vigtigt at bemærke, at EU-Domstolens besvarelse kun omfatter den situation, hvor internetudbyderen (webhoteltjenesten bag den pågældende hjemmeside) er etableret i EU.[673]

6.1.2.3.2. Datatilsynet har endvidere i en sag, Datatilsynets j.nr. 2007-214-0004, hvor ATP ønskede at overføre oplysninger om sine medlemmer til databehandlere i Indien og Sydafrika, bl.a. udtalt, at der efter tilsynets opfattelse er tale om en overførsel til et tredjeland i persondatalovens § 27's forstand, selvom en databehandler udelukkende vil kunne se de

[671] EU-Domstolens dom af 6. november 2003.
[672] Se dommens præmisser 68 og 69.
[673] Se Persondataloven med kommentarer (2015), s. 449.

oplysninger, der på et givent tidspunkt befinder sig på vedkommendes skærm, og selvom databehandleren ikke vil kunne lagre eller printe de pågældende oplysninger.

I sagen bliver det således fastslået, at en såkaldt "se-adgang" til personoplysninger er nok til at udgøre en overførsel af personoplysninger til et tredjeland.

6.1.2.4. Overførsel af personoplysninger til tredjelande skal ske under iagttagelse af særlige regler

Som nævnt ovenfor er der i persondatalovens § 27, som har sin baggrund i databeskyttelsesdirektivets artikel 25 og 26, fastsat nærmere regler for, hvornår der må overføres personoplysninger til et tredjeland.

Udgangspunktet i persondatalovens § 27, stk. 1, er, at der ikke må overføres personoplysninger til et tredjeland, med mindre dette tredjeland sikrer et tilstrækkeligt beskyttelsesniveau (såkaldte sikre tredjelande). Dette udgangspunkt bliver dog fraveget med bestemmelserne i persondatalovens § 27, stk. 3 og 4, hvorefter der i visse situationer alligevel kan ske overførsel af personoplysninger til tredjelande, der ikke sikrer et tilstrækkeligt beskyttelsesniveau.

For en nærmere gennemgang af de enkelte bestemmelser i persondatalovens § 27 henvises der til afsnit 6.2. om overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, artikel 45, afsnit 6.3. om overførsler omfattet af fornødne garantier, artikel 46, afsnit 6.4. om bindende virksomhedsregler, artikel 47 og afsnit 6.6. om undtagelser i særlige situationer, artikel 49.

Ovennævnte gør sig i øvrigt også i vidt omfang gældende i forbindelse med såkaldte videreoverførsler, hvor en dataimportør i et tredjeland, som har modtaget oplysninger fra en dataeksportør i Danmark, ønsker at videreoverføre de modtagne personoplysninger til en ny dataimportør i et tredjeland.

Hvis oplysningerne overføres til en dataimportør i et tredjeland, der alene skal fungere som databehandler for den danske dataeksportør, skal reglerne i § 27 altid iagttages ved videreoverførsler, jf. herved også reglerne i persondatalovens § 42.

Overføres oplysningerne til en dataansvarlig dataimportør i et tredjeland, skal reglerne i § 27 iagttages ved videreoverførsler, hvis det oprindelige overførselsgrundlag er persondatalovens § 27, stk. 4, jf. bl.a. side 33 ff. i EU-Kommissionens FAQ om overførsel til tredjelande (baseret på EU-Kommissionens standardkontrakter) og Artikel 29-gruppens udtalelse

af 3. juni 2003 om brug af såkaldte bindende virksomhedsregler ved overførsel til tredjelande (WP 74), s. 9.

Hvis oplysningerne overføres til en dataansvarlig dataimportør i et tredjeland i medfør af persondatalovens § 27, stk. 1, skal reglerne i persondatalovens § 27 ikke iagttages ved videreoverførsler. I stedet skal det pågældende tredjelands overførselsregler iagttages. Det er i den forbindelse vigtigt at være opmærksom på, at tredjelande, der har modtaget en tilstrækkelighedsafgørelse fra EU-Kommissionen (og derfor er at betragte som sikre tredjelande efter persondatalovens § 27, stk. 1), skal have regler og praksisser, der i det væsentlige svarer til det beskyttelsesniveau, der gælder i EU.

Overføres oplysningerne til en dataansvarlig dataimportør i et tredjeland i medfør af persondatalovens § 27, stk. 3, er der ingen regler, der specifikt regulerer muligheden for videreoverførsel. Er hjemlen samtykke, jf. § 27, stk. 3, nr. 1, vil en videreoverførsel dog formentlig skulle kunne rummes i det afgivne samtykke. Det skal bemærkes, at Artikel 29-gruppen ad flere omgange har udtalt, at undtagelserne i persondatalovens § 27, stk. 3, skal fortolkes restriktivt, således at undtagelsen ikke bliver en regel.[674]

Om baggrunden for, hvorfor det skal være muligt at overføre personoplysninger til tredjelande, der sikrer et tilstrækkeligt beskyttelsesniveau, fremgår det af databeskyttelsesdirektivets præambelbetragtning nr. 56 bl.a., at strømmen af personoplysninger på tværs af landegrænserne er nødvendig af hensyn til udbygningen af den internationale samhandel.

6.1.2.5. De øvrige regler finder anvendelse

Det følger af persondatalovens § 27, stk. 6, at en overførsel af personoplysninger til tredjelande altid skal ske inden for rammerne af persondataloven. Dette indebærer bl.a., at der skal være hjemmel til behandlingen i lovens kapitel 4-6, og at reglerne for anmeldelse skal iagttages.

Når man overfører personoplysninger til tredjelande, skal man således både have hjemmel til overførslen (§ 27) og til behandlingen i øvrigt (§§ 5, 6, 7 og 8 mv.). Der er med andre ord tale om et dobbelt hjemmelskrav.

Det fremgår af Registerudvalgets betænkning nr. 1345, at bestemmelsen har baggrund i den antagelse, at ordningen i databeskyttelsesdirektivets artikel 25 og 26 bygger på den forudsætning, at overførsel til tredjelande kun kan ske, hvis de nationale bestemmelser, der vedtages til gennemførelse af direktivets øvrige bestemmelser, overholdes. For så vidt an-

[674] Se f.eks. Artikel 29-gruppens udtalelse af 25. november 2005 om en ensartet fortolkning af artikel 26, stk. 1, i databeskyttelsesdirektivet (WP 114), s. 7.

går overførsel til et tredjeland, som sikrer et tilstrækkeligt beskyttelsesniveau, fremgår dette udtrykkeligt af bestemmelsen i artikel 25, stk. 1, 2. pkt. Tilsvarende fremgår det direkte af bestemmelserne i artikel 26, men må dog ifølge Registerudvalget antages at følge af den omstændighed, at der må antages at skulle stilles mindst samme krav til en overførsel til et tredjeland, som ikke sikrer et tilstrækkeligt beskyttelsesniveau, som til et tredjeland, der gør det. Denne antagelse bestyrkes ifølge Registerudvalget også af, at det af direktivets præambelbetragtning nr. 60 fremgår, at overførsel under alle omstændigheder kun må finde sted under fuld overholdelse af de bestemmelser, som medlemsstaterne vedtager i medfør af direktivet, særligt artikel 8.[675]

6.1.2.6. Artikel 29-gruppens fire essentielle europæiske garantier, der altid skal iagttages ved overførsel af personoplysninger til tredjelande

Den 6. oktober 2015 erklærede EU-Domstolen den tidligere Safe Harbor-ordning for ugyldig i den såkaldte Schrems-sag.

EU-Domstolen stillede i Schrems-sagen bl.a. spørgsmålstegn ved omfanget af de amerikanske myndigheders mulighed for – af hensyn til national sikkerhed og retshåndhævelse – at gøre indgreb i europæiske registreredes fundamentale rettigheder. Ifølge EU-Domstolen, må sådanne indgreb ikke gå videre, end hvad der er nødvendigt i et demokratisk samfund.

Da de amerikanske myndigheders mulige indgreb ikke var begrænset til oplysninger overført på baggrund af Safe Harbor-ordningen, blev der også stillet spørgsmålstegn ved, om de øvrige overførselsgrundlag (EU-Kommissionens standardkontraktbestemmelser, bindende virksomhedsregler mv.[676]) sikrer tilstrækkelige garantier for de registrerede, når deres personoplysninger overføres til USA.

På denne baggrund valgte Artikel 29-gruppen i efteråret 2015 at iværksætte en omfattende analyse af, hvilke garantier, der skal være på plads for at sikre, at indgreb i de registreredes fundamentale rettigheder ikke går videre, end hvad der er nødvendigt i et demokratisk samfund, når der overføres oplysninger til USA (og andre tredjelande).

Dette analysearbejde har bl.a. resulteret i, at Artikel 29-gruppen i en udtalelse[677] af 13. april 2016 har opstillet fire essentielle europæiske garantier, der *altid* skal iagttages ved overførsel af personoplysninger til tredjelande.

[675] Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 285.
[676] Se afsnit 6.3. om overførsel omfattet af fornødne garantier og afsnit 6.4. om bindende virksomhedsregler.
[677] Se Artikel 29-gruppens udtalelse om berettigelsen af indgreb i den fundamentale ret til privacy og databeskyttelse gennem overvågningsforanstaltninger ved overførsel af personoplysninger (WP 237).

De fire essentielle europæiske garantier, der er udledt af praksis fra EU-Domstolen og Den Europæiske Menneskerettighedsdomstol, har følgende indhold:

1. Myndigheders adgang til personoplysninger skal ske på grundlag af klare, præcise og tilgængelige regler.
2. Myndighedernes adgang til og brug af personoplysninger skal være nødvendig og proportional (der skal være balance mellem formålet (national sikkerhed) og indgrebet i de registreredes ret til beskyttelse af deres privatliv).
3. Der skal være en uafhængig og effektiv tilsynsmyndighed.
4. Der skal være tilgængelige og effektive retsmidler for de registrerede.

Konsekvensen af de fire essentielle europæiske garantier er i princippet, at der ikke kan overføres personoplysninger om europæiske registrerede til et tredjeland, hvis dette tredjelands lovgivning, praksisser mv., i forhold til offentlige myndigheders mulighed for at tilgå oplysninger af hensyn til national sikkerhed og retshåndhævelse, ikke muliggør en efterlevelse af garantierne.

6.1.3. Databeskyttelsesforordningen

Det fremgår af databeskyttelsesforordningens artikel 44, 1. pkt, at enhver overførsel af personoplysninger, som underkastes behandling eller planlægges behandlet efter overførsel til et tredjeland eller en international organisation, kun må finde sted, hvis betingelserne i forordningens kapitel V – med forbehold af de øvrige bestemmelser i forordningen – opfyldes af den *dataansvarlige* og *databehandleren*, herunder ved videreoverførsel af personoplysninger fra det pågældende tredjeland eller den pågældende internationale organisation til et andet tredjeland eller en anden international organisation.

Endvidere fremgår det af databeskyttelsesforordningens artikel 44, 2. pkt., at alle bestemmelserne i kapitel V anvendes for at sikre, at det beskyttelsesniveau, som fysiske personer garanteres i medfør af forordningen, ikke undermineres.

Af præambelbetragtning nr. 101 fremgår det, at strømmen af personoplysninger til og fra lande uden for Unionen og til og fra internationale organisationer er nødvendig af hensyn til udbygningen af den internationale samhandel og det internationale samarbejde. Det fremgår tillige, at udvidelsen af denne strøm har skabt nye udfordringer og betænkeligheder med hensyn til beskyttelsen af personoplysninger. Herudover fremgår det, at når personoplysninger overføres fra Unionen til dataansvarlige, databehandlere eller andre modta-

gere i tredjelande eller til internationale organisationer, må det beskyttelsesniveau, som fysiske personer sikres i Unionen i medfør af denne forordning, dog ikke undermineres, herunder i tilfælde af videreoverførsel af personoplysninger fra et tredjeland eller en international organisation til dataansvarlige, databehandlere i det samme eller et andet tredjeland eller en anden international organisation. Om betingelserne for at overføre personoplysninger til tredjelande fremgår det, at overførsel til tredjelande og internationale organisationer under alle omstændigheder kun må finde sted under fuld overholdelse af forordningen. Endelig fremgår det, at en overførsel således kun vil kunne finde sted, hvis den dataansvarlige eller databehandleren opfylder betingelserne i denne forordning vedrørende overførsel af personoplysninger til tredjelande eller internationale organisationer, jf. dog de øvrige bestemmelser i denne forordning.

6.1.4. Overvejelser

I præambelbetragtninger til både databeskyttelsesdirektivet og databeskyttelsesforordningen bliver det fastslået, at strømmen af personoplysninger til og fra lande uden for EU er nødvendig af hensyn til den internationale samhandel.

Det bliver endvidere i både persondataloven og i databeskyttelsesforordningen fastslået, at der kun kan ske overførsel af personoplysninger til et tredjeland, hvis de i loven (§ 27) og forordningen (kapitel 5) særlige bestemmelser herom bliver iagttaget.

Ligeledes fremgår det af både persondataloven (§ 27, stk. 6) og databeskyttelsesforordningen (artikel 44), at henholdsvis lovens og forordningens øvrige regler skal iagttages ved overførsel af personoplysninger til tredjelande. Dette indebærer f.eks., at persondatalovens og forordningens behandlingsregler skal iagttages.

Når det i databeskyttelsesforordningens artikel 44 bliver fastslået, at det generelle princip også skal iagttages ved videreoverførsel fra det pågældende tredjeland eller den pågældende internationale organisation til et andet tredjeland eller en anden international organisation (i et tredjeland) er dette også i vidt omfang udtryk for en videreførelse af gældende ret. Der henvises i den forbindelse til afsnit 6.2. om overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, artikel 45, afsnit 6.3. om overførsler omfattet af fornødne garantier, artikel 46, afsnit 6.4. om bindende virksomhedsregler, artikel 47 og afsnit 6.6. om undtagelser i særlige situationer, artikel 49.

Herudover vil de fire essentielle europæiske garantier – både i dag og når forordningen finder anvendelse – skulle iagttages ved overførsel af personoplysninger til tredjelande.

Det at der i databeskyttelsesforordningens artikel 44 henvises til både tredjelande og internationale organisationer kan ikke – i forhold til det generelle princip – antages at have en indholdsmæssig betydning, men er alene udtryk for en sproglig præcisering. I den sammenhæng må det samtidig kunne lægges til grund, at forordningens kapitel V kun finder anvendelse i forhold til overførsler til internationale organisationer, der befinder sig i et tredjeland.

På denne baggrund kan det konkluderes, at det generelle princip i databeskyttelsesforordningens artikel 44 stort set er en videreførelse af gældende ret. Det fremhæves, at det fremgår af ordlyden af artikel 44, at pligten til at sikre lovlig tredjelandsoverførsel hviler på "den dataansvarlige og databehandleren".

6.2. Overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, artikel 45

6.2.1. Præsentation

Efter persondatalovens § 27, stk. 1, må der som udgangspunkt kun overføres personoplysninger til et tredjeland, hvis dette land sikrer et tilstrækkeligt beskyttelsesniveau. Det følger samtidig af § 27, stk. 2, hvad der skal lægges vægt på ved vurderingen af, om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau. Bestemmelserne i persondatalovens § 27, stk. 1 og 2, har sin baggrund i artikel 25, stk. 1 og 2, i databeskyttelsesdirektivet.

Databeskyttelsesforordningens artikel 45 indeholder regler, der minder om de gældende regler i persondataloven og databeskyttelsesdirektivet.

6.2.2. Gældende ret

6.2.2.1. Persondatalovens § 27, stk. 1

Det fremgår af persondatalovens § 27, stk. 1, at der kun må overføres personoplysninger til et tredjeland, hvis dette land sikrer et tilstrækkeligt beskyttelsesniveau.

Bestemmelsen har, som nævnt ovenfor, sin baggrund i databeskyttelsesdirektivets artikel 25, stk. 1, hvoraf det fremgår, at medlemsstaterne fastsætter bestemmelser om, at videregivelse til et tredjeland af personoplysninger, der gøres til genstand for behandling, eller som skal gøres til genstand for behandling efter videregivelsen, kun må finde sted, hvis det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, og forudsat at de nationale bestemmelser, der vedtages til gennemførelse af direktivets øvrige bestemmelser, overholdes. For nærmere om begrebet "tredjeland" og forskellen i ordlyden mellem persondatalo-

vens § 27, stk. 1 (”overførsel”), og databeskyttelsesdirektivets artikel 25, stk. 1 (”videregivelse”) henvises til afsnit 6.1.2.2.

Af direktivets præambelbetragtning nr. 56 fremgår det bl.a., at den beskyttelse, der ved direktivet garanteres personer inden for Fællesskabet, ikke er til hinder for, at der videregives personoplysninger til tredjelande, for så vidt disse sikrer et tilstrækkeligt beskyttelsesniveau.

Samtidig fremgår det modsætningsvist af præambelbetragtning nr. 57, at hvis et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau, skal videregivelse af oplysninger til det pågældende land forbydes.

Efter ordlyden i persondatalovens § 27, stk. 1, er det som udgangspunkt et *helt* tredjeland, der kan sikre et tilstrækkeligt beskyttelsesniveau.

I teorien har man dog også accepteret muligheden for, at f.eks. sektorer eller delstater (i et land med føderal opbygning) i et tredjeland partielt skal kunne konstateres som sikrende et tilstrækkeligt beskyttelsesniveau.[678]

Denne teori har udmøntet sig til praksis i forhold til Kommissionens tilstrækkelighedsafgørelser[679] med hensyn til Canada og USA, hvorefter der i medfør af persondatalovens § 27, stk. 1, kan ske overførsel af personoplysninger til organisationer i det pågældende land, der er underlagt eller har tilsluttet sig et givent databeskyttelsesretligt regelsæt (PIPED Act og EU-U.S. Privacy Shield).

Af bemærkningerne til persondatalovens § 27, stk. 1, fremgår det, at der i kravet om, at et tredjeland skal sikre et tilstrækkeligt beskyttelsesniveau, ligger, at overførslen af oplysninger ikke må medføre en væsentlig forringelse af den beskyttelse af den registrerede, som loven tilsigter at sikre. Endvidere fremgår det, at behandlingen i det pågældende tredjeland således i det væsentlige skal være undergivet en regulering som den, der følger af loven. For så vidt angår kravet om, at behandlingen i det pågældende tredjeland i det væsentlige skal være undergivet en regulering som den, der følger af persondataloven fremgår det, at dette dels gælder for så vidt angår de materielle krav til behandling af oplysninger, herunder reglerne om den registreredes rettigheder, og dels for så vidt angår de formelle krav om

[678] Se Artikel 29-gruppens udtalelse af 24. juli 1998 (WP 12), s. 28 og Peter Blume, Retlig regulering af internationale persondataoverførsler, 1. udgave (2006), s. 91-92.
[679] EU-Kommissionens afgørelser af 20. december 2001 (2002/2/EF) og afgørelse af 12. juli 2016 (C(2016) 4176 final).

bl.a. tilsyn og behandlingssikkerhed og muligheden for via domstolene at få kontrolleret overholdelsen af reglerne. [680]

I persondataloven med kommentarer[681] anføres det – i lighed med hvad der har været den gængse opfattelse blandt mange aktører på databeskyttelsesområdet – at "det synes dog tvivlsomt, om dette høje ambitionsniveau (behandlingen skal i det væsentlige være undergivet en regulering som den, der følger af persondataloven) fuldt ud vil kunne fastholdes i praksis."

Det skal i den forbindelse bemærkes, at kommentaren til persondataloven er skrevet før EU-Domstolen afsagde dom i den såkaldte Schrems-sag[682] den 6. oktober 2015. Med dommen erklærede EU-Domstolen den tidligere Safe Harbor-ordning ugyldig. Safe Harbor-ordningen var en aftale mellem EU og USA om, at amerikanske organisationer, der havde tilsluttet sig ordningen, var at betragte som havende et tilstrækkeligt beskyttelsesniveau i medfør af persondatalovens § 27, stk. 1 (direktivets artikel 25, stk. 1). EU-Kommissionen havde i overensstemmelse med aftalen – i medfør af databeskyttelsesdirektivets artikel 25, stk. 6 – truffet afgørelse[683] om, at overførsler til disse organisationer var tilstrækkeligt sikkert.

EU-Domstolen udtalte i dommen bl.a. følgende i præmis 73:

"Ordet "tilstrækkeligt", der er indeholdt i artikel 25, stk. 6, i databeskyttelsesdirektivet, indebærer ganske vist, at det ikke kan kræves, at et tredjeland sikrer et beskyttelsesniveau, som er identisk med det niveau, som er sikret i Unionens retsorden. Som anført af generaladvokaten i punkt 141 i forslaget til afgørelse, skal udtrykket "et tilstrækkeligt beskyttelsesniveau" imidlertid forstås således, at det opstiller et krav om, at dette tredjeland på grundlag af dets nationale lovgivning eller dets internationale forpligtelser faktisk sikrer et beskyttelsesniveau for frihedsrettighederne og de grundlæggende rettigheder, *som i det væsentlige svarer til det niveau, der er sikret inden for Unionen i medfør af direktiv 95/46, sammenholdt med chartret*. Såfremt der ikke blev opstillet et sådant krav, ville det mål, som er anført i denne doms foregående præmis, være tilsidesat. Desuden ville det høje beskyttelsesniveau, der er sikret ved databeskyttelsesdirektivet, sammenholdt med chartret, let kunne omgås ved videregivelse af personoplysninger fra Unionen til tredjelande med henblik på behandling heraf i disse lande."

[680] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00.
[681] Persondataloven med kommentarer (2015), s. 446.
[682] Sag C-362/14 – Maximillian Schrems mod Data Protection Commissioner (det irske datatilsyn).
[683] EU-Kommissionens afgørelse 2000/520/EF af 26. juli 2000.

EU-Domstolen fastlægger således en linje i forhold til tilstrækkelighedsvurderingen, som minder om den, der fremgår af bemærkningerne til persondatalovens § 27, stk. 1. Det "høje ambitionsniveau" skal derfor fastholdes i praksis.

Det må derfor kunne forventes, at EU-Kommissionen – ved fremtidige vurderinger af om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau – vil have EU-Domstolens udtalelse i Schrems-sagen in mente, og at tilstrækkelighedsvurderingen som følge heraf måske vil blive skærpet. Hvis vurderingen bliver skærpet, kan dette også få betydning for tredjelande, hvor EU-Kommissionen allerede har truffet afgørelse om, at de sikrer et tilstrækkeligt beskyttelsesniveau, jf. mere herom nedenfor.

Umiddelbart må det antages, at det vil være meget få tredjelande, der har et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er sikret inden for Unionen i medfør af databeskyttelsesdirektivet sammenholdt med Den Europæiske Unions Charter om Grundlæggende Rettigheder (se især artikel 7, 8 og 47).

At det formentlig er meget få tredjelande, der kan anses for at sikre et tilstrækkeligt beskyttelsesniveau blev allerede understreget af Artikel 29-gruppen i en udtalelse af 24. juli 1998 om videregivelse af personoplysninger til tredjelande (WP 12). Udtalelsen fra EU-Domstolen i Schrems-sagen, som også inddrager chartret, vil næppe lette processen for de tredjelande, der måtte ønske at få en tilstrækkelighedsafgørelse fra EU-Kommissionen.

6.2.2.2. Persondatalovens § 27, stk. 2

Af persondatalovens § 27, stk. 2, fremgår det, at vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, sker på grundlag af samtlige de forhold, der har indflydelse på en overførsel, herunder navnlig oplysningernes art, behandlingens formål og varighed, oprindelseslandet og det endelige bestemmelsesland, samt de retsregler, regler for god forretningsskik og sikkerhedsforanstaltninger, der gælder i tredjelandet.

Bestemmelsen har sin baggrund i artikel 25, stk. 2, i databeskyttelsesdirektivet, hvoraf det fremgår, at vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, sker på grundlag af samtlige de forhold, der har indflydelse på en videregivelse eller en type videregivelse af oplysninger; til grund for vurderingen lægges navnlig oplysningernes art, den eller de påtænkte behandlingers formål og varighed, oprindelseslandet og det endelige bestemmelsesland, de retsregler – almindelige regler eller sektorregler – der er i kraft i det pågældende tredjeland, samt de regler for god forretningsskik og de sikkerhedsforanstaltninger, der gælder i landet.

Det fremgår af bemærkningerne til persondatalovens § 27, stk. 2, at opregningen af faktorer, som der kan lægges vægt på, ikke er udtømmende, og at der således kan være andre faktorer, som kan indgå i vurderingen af, om et tredjeland har et tilstrækkeligt beskyttelsesniveau. Af bemærkningerne fremgår det tillige, at der ved vurderingen af, om beskyttelsesniveauet er tilstrækkeligt, skal lægges afgørende vægt på oplysningernes art i de tilfælde, hvor der er tale om offentliggørelse af personoplysninger, herunder gennem internettet.

Artikel 29-gruppen har i ovennævnte udtalelse fra 1998 (WP 12) bl.a. udtalt sig om, hvori en tilstrækkelig beskyttelse består.

Artikel 29-gruppen udtaler således, at formålet med databeskyttelse er at yde beskyttelse af den person, om hvem der behandles oplysninger. Artikel 29-gruppen udtaler endvidere, at dette typisk opnås gennem en kombination af rettigheder, der tildeles den registrerede, og forpligtelser, der pålægges dem, der behandler oplysninger, eller dem, der fører tilsyn med behandlingen. Forpligtelserne og rettighederne i databeskyttelsesdirektivet bygger, ifølge Artikel 29-gruppen, på de forpligtelser og rettigheder, der er fastsat i Europarådets konvention 108 (1981), som på sin side ikke er væsensforskellige fra dem, der er fastsat i OECD's retningslinjer (1980) eller FN's retningslinjer (1990). Ifølge Artikel 29-gruppen lader det derfor til, at der er en grad af konsensus om indholdet af databeskyttelsesreglerne, som rækker langt ud over de femten EU-medlemsstater.

Artikel 29-gruppen udtaler endvidere, at databeskyttelsesregler dog kun bidrager til beskyttelsen af personer, hvis de overholdes i praksis. Af den grund er det, ifølge Artikel 29-gruppen, ikke blot nødvendigt at se på indholdet af de regler, der gælder for videregivelse af personoplysninger til tredjelande, men også det system, der er indført for at sikre, at reglerne overholdes. Artikel 29-gruppen anfører endvidere, at der i Europa historisk har været en tendens til at fastsætte databeskyttelsesreglerne ved lov, hvorved manglende overholdelse kan sanktioneres, og den enkelte kan få klageadgang. Ifølge Artikel 29-gruppen har disse love almindeligvis også omfattet yderligere proceduremekanismer, f.eks. tilsynsmyndigheder med beføjelse til at overvåge og undersøge klager. Disse proceduremæssige aspekter er, ifølge Artikel 29-gruppen, afspejlet i databeskyttelsesdirektivet i dets bestemmelser om ansvar, sanktioner, retsmidler, tilsynsmyndigheder og anmeldelse. Uden for EU er det ifølge Artikel 29-gruppen mindre almindeligt at finde sådanne proceduremæssige måder at sikre overholdelse af databeskyttelsesreglerne på. Artikel 29-gruppen nævner som eksempel, at parterne i konvention 108 skal knæsætte databeskyttelsesprincipperne i lov, men der er ikke noget krav om yderligere mekanismer som en tilsynsmyndighed. OECD's retningslinjer stiller kun krav om, at der skal "tages hensyn til dem" i den nationale lovgivning, og omfatter ingen proceduremæssige muligheder for at sikre, at retningslinjerne reelt medfører en effektiv beskyttelse af enkeltpersoner. Endelig udtaler Artikel 29-gruppen, at

de senere FN-retningslinjer derimod omfatter bestemmelser om tilsyn og sanktioner, hvilket afspejler en voksende erkendelse over hele kloden af, at det er nødvendigt, at databeskyttelsesreglerne håndhæves ordentligt.

På baggrund af ovenstående står det, ifølge Artikel 29-gruppen, klart, at hvis en analyse af, om en beskyttelse er tilstrækkelig, skal give mening, skal den omfatte to grundelementer, nemlig indholdet af gældende regler og midlerne til sikring af, at de reelt finder anvendelse.

Artikel 29-gruppen udtaler endvidere, at hvis man tager udgangspunkt i databeskyttelsesdirektivet og holder sig andre internationale databeskyttelsesbestemmelser for øje, skulle det være muligt at formulere en "kerne" af "indholdsprincipper" og "procedure-/håndhævelseskrav" for databeskyttelse, hvis overholdelse vil kunne betragtes som et minimumskrav for, at en beskyttelse kan anses for at være tilstrækkelig. En sådan minimumsliste må dog, ifølge Artikel 29-gruppen, ikke have form af en udtømmende opregning. I nogle tilfælde vil der, ifølge Artikel 29-gruppen, være behov for at føje nye elementer til listen, mens det i andre tilfælde endda vil være muligt at reducere listen af krav. Graden af risiko, som en videregivelse indebærer for den registrerede, er en vigtig faktor i forbindelse med at afgøre de præcise krav i det enkelte tilfælde. Endelig udtaler Artikel 29-gruppen, at uanset dette forbehold er opstillingen af en grundlæggende liste af minimumskrav et nyttigt udgangspunkt for analysen.

Herefter opstiller Artikel 29-gruppen en grundlæggende liste af minimumskrav, som der kan tages udgangspunkt i, når det konkret skal vurderes, om et tredjeland sikrer et tilstrækkelige beskyttelsesniveau. Listen opdeles, som nævnt ovenfor, i henholdsvis *indholdsmæssige principper* og *procedure/håndhævelseskrav.*

I forhold til de indholdsmæssige principper udtaler Artikel 29-gruppen, at der, ved afgørelsen af om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, skal ses på, om det pågældende lands gældende regler indeholder principper om 1) formålsafgrænsning, 2) datakvalitet- og dataproportionalitet, 3) gennemsigtighed (oplysning om formål med behandling), 4) sikkerhed, 5) ret til indsigt, berigtigelse og indsigelse samt 6) begrænsninger i videreoverførsler.

Herudover udtaler Artikel 29-gruppen, at der skal fastsættes yderligere principper i forhold til bestemte former for behandlinger, herunder ved behandling af oplysninger af følsom karakter, behandlinger med henblik på direkte markedsføring og behandlinger i forbindelse med edb-baserede individuelle afgørelser.

For så vidt angår procedure/håndhævelseskravene (midlerne til sikring af at de gældende regler bliver efterlevet i praksis) udtaler Artikel 29-gruppen, at der findes tre målsætninger for et databeskyttelsessystem, som et tredjelands system skal indeholde, hvis tredjelandet skal anses for at sikre et tilstrækkeligt beskyttelsesniveau. Systemerne skal ifølge Artikel 29-gruppen 1) tilvejebringe en høj grad af overholdelse (bevidsthed om forpligtelser og rettigheder), 2) yde støtte og hjælp til individuelle registrerede (skal forefindes en uafhængig institution der kan undersøge klager) og 3) yde passende genoprejsning til skadeslidte (erstatning og sanktioner).

I praksis har medlemmerne af Artikel 29-gruppen taget udgangspunkt i principperne i ovennævnte udtalelse, når EU-Kommissionen – i forbindelse med vurderingen af om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau – har bedt gruppen om en udtalelse i medfør af databeskyttelsesdirektivets artikel 30, stk. 1, litra b.

Efter de gældende regler kan en dataansvarlig – ved at tage udgangspunkt i bl.a. ovennævnte udtalelse fra Artikel 29-gruppen – i princippet selv foretage en vurdering af, om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau efter persondatalovens § 27, stk. 1. Dette gør sig navnlig gældende i situationer, hvor der ikke påtænkes overført følsomme personoplysninger, da sådanne overførsler ikke vil kræve en forudgående udtalelse fra Datatilsynet efter persondatalovens § 45, stk. 1, nr. 1 (offentlige dataansvarlige) eller en forudgående tilladelse fra tilsynet efter lovens § 50, stk. 2 (private dataansvarlige). Vurderingen vil således i disse situationer ske helt uden involvering af Datatilsynet. Det sker dog formentlig sjældent, at en dataansvarlig selv foretager en vurdering af, om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, da det er en kompliceret vurdering, der forudsætter et indgående kendskab til tredjelandets gældende lovgivning og praksisser mv.

Herudover kan EU-Kommissionen – ved at tage udgangspunkt i kriterierne i databeskyttelsesdirektivets artikel 25, stk. 2 – med bindende virkning for medlemsstaterne træffe afgørelse om, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, jf. også gennemgangen af databeskyttelsesdirektivets artikel 25, stk. 6, umiddelbart nedenfor.

6.2.2.3. Afgørelse om tilstrækkeligt beskyttelsesniveau – databeskyttelsesdirektivets artikel 25, stk. 6

Det fremgår af databeskyttelsesdirektivets artikel 25, stk. 6, at EU-Kommissionen – efter proceduren i artikel 31, stk. 2 – kan fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2. Vurderingen sker på grundlag af tredjelandets nationale lovgivning eller dets internationale forpligtelser med henblik på at beskytte privatlivet og personers grundlæggende rettigheder og frihedsrettigheder, herunder de forpligtelser, der er indgået efter de i artikel 25, stk. 5, nævnte forhandlinger mellem

EU-Kommissionen og tredjelandet. Endvidere fremgår det, at medlemsstaterne skal træffe de foranstaltninger, der er nødvendige for at efterkomme EU-Kommissionens afgørelse.

På nuværende tidspunkt har EU-Kommissionen – med bindende virkning for medlemsstaterne – truffet afgørelse om, at følgende tredjelande sikrer et tilstrækkeligt beskyttelsesniveau:

Andorra	**Argentina**
Australien (overførsel af oplysninger om flypassagerer)	**Canada** (overførsel til modtagere underlagt den canadiske Personal Information Protection and Electronic Documents Act (PIPED Act))
Færøerne	**Guernsey**
Isle of Man	**Israel**
Jersey	**New Zealand**
Schweiz	**Uruguay**
USA (overførsel af oplysninger om flypassagerer)	**USA** (overførsel til organisationer (typisk virksomheder), der har tilsluttet sig EU-U.S. Privacy Shield

Når EU-Kommissionen har truffet afgørelse om, at ovennævnte lande sikrer et tilstrækkeligt beskyttelsesniveau, indebærer det, at en dataansvarlig frit kan overføre personoplysninger til de pågældende lande uden at skulle stille yderligere garantier, forudsat at oplysningerne behandles lovligt i EU. Landene kaldes derfor i daglig tale for ”sikre tredjelande”.

Det er i dansk kontekst vigtigt at være opmærksom på, at Grønland – modsat Færøerne – ikke sikrer et tilstrækkeligt beskyttelsesniveau, hvorfor Grønland ikke er at betragte som et sikkert tredjeland. At persondataloven den 1. december 2016 blev sat i kraft for Grønland ændrer ikke herpå.

Til trods for at der som udgangspunkt frit kan overføres personoplysninger til sikre tredjelande, skal danske dataansvarlige dog være opmærksomme på, at de – hvis de ønsker at overføre følsomme personoplysninger til et af de sikre tredjelande – skal have en forudgående udtalelse (offentlige dataansvarlige) eller tilladelse (private dataansvarlige) fra Datatilsynet.

For en nærmere gennemgang af den procedure, som EU-Kommissionen skal følge ved vurderingen af, om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau (indhentelse af

udtalelse fra Artikel 29-gruppen og Artikel 31-udvalget[684]), henvises til persondataloven med kommentarer.[685]

6.2.2.4. Udviklingen i et tredjeland med et tilstrækkeligt beskyttelsesniveau

Persondataloven og databeskyttelsesdirektivet indeholder ingen specifikke regler om, at udviklingen i et tredjeland skal følges, når EU-Kommissionen har truffet afgørelse om, at det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau.

Det følger imidlertid af EU-Kommissionens tilstrækkelighedsafgørelser, at EU-Kommissionen skal føre tilsyn med anvendelsen heraf.

I de tilstrækkelighedsafgørelser, der er fra før 2015, fremgår der ikke noget nærmere om, hvordan EU-Kommissionen skal føre tilsyn og hvor ofte mv.[686]

Derimod fremgår det udtrykkeligt af artikel 4 i EU-Kommissionens tilstrækkelighedsafgørelse vedrørende EU-U.S. Privacy Shield, at EU-Kommissionen vedvarende skal overvåge, at EU-U.S. Privacy Shield'et fungerer som det skal, og at EU-Kommissionen samtidig skal overvåge, om USA vedbliver med at sikre et tilstrækkeligt beskyttelsesniveau. Herudover fremgår det udtrykkeligt, at EU-Kommissionen årligt skal evaluere sin tilstrækkelighedsafgørelse.

Når tilstrækkelighedsafgørelsen, vedrørende EU-U.S. Privacy Shield, er anderledes end de øvrige tilstrækkelighedsafgørelser, skyldes dette, at førstnævnte er blevet vedtaget i forlængelse af føromtalte dom fra EU-Domstolen i Schrems-sagen. I dommen udtalte EU-Domstolen bl.a. i præmis 76, at:

"Henset til den omstændighed, at det beskyttelsesniveau, som et tredjeland sikrer, kan ændre sig, påhviler det endvidere Kommissionen efter vedtagelse af en afgørelse i henhold til artikel 25, stk. 6, i databeskyttelsesdirektivet at undersøge med regelmæssige mellemrum, om konstateringen vedrørende det tilstrækkelige beskyttelsesniveau, som er sikret i det pågældende tredjeland, stadig er faktisk og retligt begrundet. En sådan undersøgelse skal under alle omstændighed foretages, når oplysninger bevirker, at der opstår tvivl i denne henseende."

EU-Kommissionen har således i sin tilstrækkelighedsafgørelse vedrørende EU-U.S. Privacy Shield taget højde for EU-Domstolens udtalelse i Schrems-sagen.

---

[684] Artikel 31-udvalget (direktivets artikel 31) består af repræsentanter for medlemsstaternes regeringer.
[685] Persondataloven med kommentarer (2015), s. 449-450.
[686] Se f.eks. artikel 4 i EU-Kommissionens tilstrækkelighedsafgørelse vedrørende New Zealand.

I lyset af dommen må det endvidere kunne forventes, at EU-Kommissionen i et eller andet omfang vil iværksætte en lignende procedure i forhold til de øvrige tilstrækkelighedsafgørelser. Kommissionen er dog indtil videre ikke kommet med udmeldinger herom.

6.2.2.5. Hvis et tredjeland ikke (længere) sikrer et tilstrækkeligt beskyttelsesniveau – databeskyttelsesdirektivets artikel 25, stk. 3 og 4

Af databeskyttelsesdirektivets artikel 25, stk. 3, fremgår det, at medlemsstaterne og EU-Kommissionen gensidigt underretter hinanden, hvis de mener, at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2.

Endvidere fremgår det af direktivets artikel 25, stk. 4, at hvis EU-Kommissionen, efter proceduren i artikel 31, stk. 2, konstaterer, at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2, skal medlemsstaterne træffe de foranstaltninger, der er nødvendige for at hindre enhver overførsel af oplysninger af samme art til det pågældende tredjeland.

Direktivets artikel 25, stk. 4, er gennemført i dansk ret ved persondatalovens § 58, stk. 2, hvoraf det fremgår, at Datatilsynet til enhver tid bl.a. kan tilbagekalde en afgørelse truffet i henhold til § 50, stk. 2, jf. § 27, stk. 1 (tilladelse til at en privat dataansvarlig kan overføre følsomme personoplysninger til et sikkert tredjeland), hvis EU-Kommissionen træffer afgørelse om, at der ikke må ske overførsel af oplysninger til bestemte tredjelande, eller om, at der lovligt kan ske en sådan overførsel. Endvidere fremgår det, at dette dog kun gælder, såfremt tilbagekaldelsen er nødvendig for at efterleve Kommissionens afgørelse.

I praksis har det været overvejet at benytte reglen i persondatalovens § 58, stk. 2, i forbindelse med ovenfor omtalte Schrems-sag. Datatilsynet havde forud for dommen givet en række virksomheder m.fl. tilladelse til at overføre følsomme personoplysninger til organisationer i USA, der havde tilsluttet sig Safe Harbor-ordningen.

Det blev imidlertid vurderet, at det ikke var nødvendigt med en egentlig tilbagekaldelse af de meddelte tilladelser, idet EU-Domstolen havde erklæret hele Safe Harbor-ordningen for ugyldig. Udstedte tilladelser efter persondatalovens § 50, stk. 2, jf. § 27, stk. 1, var således en nullitet, der ikke kunne støttes ret på. Datatilsynet valgte derfor i stedet at orientere de berørte parter om dommen.

Herudover tillægges de nationale tilsynsmyndigheder – i EU-Kommissionens tilstrækkelighedsafgørelser – kompetence til at suspendere overførsler til konkrete modtagere i et tredjeland, herunder f.eks. hvis modtageren overtræder de regler, der lå til grund for Kom-

missionens tilstrækkelighedsafgørelse.[687] Dette er i overensstemmelse med databeskyttelsesdirektivets artikel 28, stk. 3, hvorefter tilsynsmyndighederne bl.a. midlertidigt eller definitivt skal kunne forbyde en behandling.

I Schrems-sagen fastslog EU-Domstolen endvidere, at nationale tilsynsmyndigheder er forpligtet til at efterprøve EU-Kommissionens tilstrækkelighedsafgørelser, når en registreret indgiver en klage. Dog kan hverken en national tilsynsmyndighed eller en national domstol erklære en tilstrækkelighedsafgørelse fra EU-Kommissionen for ugyldig. I stedet må en national tilsynsmyndighed – hvis klagen vurderes velbegrundet – anlægge en sag ved sine nationale domstole med henblik på at få spørgsmålet indbragt præjudicielt for EU-Domstolen, der er enekompetent til at fastslå ugyldigheden af en EU-retsakt.[688]

Som følge af Schrems-sagen har EU-Kommissionen i øvrigt også i efteråret 2016 foretaget ændringer af sine vedtagne tilstrækkelighedsafgørelser, således, at de nationale tilsynsmyndigheders mulighed for at efterprøve afgørelserne bliver tydeliggjort.

6.2.2.6. Afhjælpning af situationen - databeskyttelsesdirektivets artikel 25, stk. 5

Af databeskyttelsesdirektivets artikel 25, stk. 5, fremgår det, at EU-Kommissionen på det rette tidspunkt indleder forhandlinger med henblik på at afhjælpe den situation, der er opstået som følge af en konstatering efter artikel 25, stk. 4.

Et eksempel herpå kunne være EU-Kommissionens forhandlinger med de amerikanske myndigheder i forlængelse af Schrems-sagen, hvor EU-Domstolen havde erklæret den tidligere Safe Harbor-ordning ugyldig. Disse forhandlinger, der også havde pågået inden dommen fra EU-Domstolen, mundede den 12. juli 2016 ud i et nyt EU-U.S. Privacy Shield.

6.2.2.7. En afgørelse efter databeskyttelsesdirektivets artikel 25, stk. 4's betydning for andre overførselsgrundlag

Der står ikke noget specifikt i persondataloven eller databeskyttelsesdirektivet om, hvilken betydning det måtte få for andre overførselsgrundlag, at EU-Kommissionen efter databeskyttelsesdirektivets artikel 25, stk. 4, træffer afgørelse om, at et tredjeland ikke længere sikrer et tilstrækkeligt beskyttelsesniveau. Med andre overførselsgrundlag tænkes der f.eks. på EU-Kommissionens standardkontrakter eller bindende virksomhedsregler. Se mere herom i afsnit 6.3. om fornødne garantier, artikel 46 og afsnit 6.4. om bindende virksomhedsregler, artikel 47.

[687] Se f.eks. artikel 3 og 4 i EU-Kommissionens tilstrækkelighedsafgørelse vedrørende Færøerne eller artikel 3 i EU-Kommissionens tilstrækkelighedsafgørelse vedrørende EU-U.S. Privacy Shield.
[688] Se bl.a. dommens præmis 38-66.

I den sammenhæng skal det bemærkes, at overførsler baseret på EU-Kommissionens standardkontrakter og bindende virksomhedsregler sker med hjemmel i persondatalovens § 27, stk. 4, som har baggrund i databeskyttelsesdirektivets artikel 26. Persondatalovens § 27, stk. 4, vedrører overførsler til tredjelande, der ikke sikrer et tilstrækkeligt beskyttelsesniveau, og overførslerne kan efter bestemmelsen kun ske, hvis den dataansvarlige, i forbindelse med den konkrete overførsel, yder tilstrækkelige garantier for beskyttelse af de registreredes rettigheder.

De tilstrækkelige garantier, der skal stilles efter persondatalovens § 27, stk. 4, må således alt andet lige være mindre omfattende end dem, der skal stilles efter persondatalovens § 27, stk. 1, når det skal fastslås, om et helt land har et tilstrækkeligt beskyttelsesniveau. På denne baggrund må det kunne konkluderes, at en afgørelse fra EU-Kommissionen efter databeskyttelsesdirektivets artikel 25, stk. 4, ikke nødvendigvis behøver at få betydning for overførsler baseret på andre overførselsgrundlag.

Hvis EU-Kommissionens afgørelse efter databeskyttelsesdirektivets artikel 25, stk. 4, derimod f.eks. skyldes, at det berørte tredjelands myndigheder har indført regler om, at myndighederne – af hensyn til statens sikkerhed mv. – kan masseindsamle oplysninger om europæiske registrerede, som bliver behandlet af modtagere i tredjelandet, kan det ikke afvises, at EU-Kommissionens afgørelse også vil have betydning for de øvrige overførselsgrundlag. Dette må vurderes konkret, hvilket også var de europæiske tilsynsmyndigheder og EU-Kommissionens tilgang i forlængelse af EU-Domstolens dom i Schrems-sagen, hvor det bl.a. var blevet statueret, at de amerikanske myndigheder foretog masseindsamlinger af oplysninger om europæere.

6.2.2.8. Offentliggørelse af afgørelser om tilstrækkelighed

I dag findes der hverken i persondataloven eller i databeskyttelsesdirektivet specifikke regler om offentliggørelse i Den Europæiske Unions Tidende af EU-Kommissionens afgørelser om, at et givent tredjeland sikrer et tilstrækkeligt beskyttelsesniveau.

En sådan offentliggørelse[689] i Den Europæiske Unions Tidende sker i dag med udgangspunkt i artikel 297 i Traktaten om Den Europæiske Unions Funktionsmåde.

Herudover offentliggør Kommissionen også i dag sine afgørelser om, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau på sin hjemmeside.

[689] Se f.eks. EU-Kommissionens beslutning vedrørende Andorra

6.2.3. Databeskyttelsesforordningen

6.2.3.1. Databeskyttelsesforordningens artikel 45, stk. 1

Det fremgår af databeskyttelsesforordningens artikel 45, stk. 1, at overførsel af personoplysninger til et tredjeland eller en international organisation kan finde sted, hvis EU-Kommissionen har fastslået, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation har et tilstrækkeligt beskyttelsesniveau. Endvidere fremgår det, at en sådan overførsel ikke kræver specifik godkendelse.

Af præambelbetragtning nr. 103 fremgår det, at EU-Kommissionen, med virkning for hele Unionen, kan træffe afgørelse om, at et tredjeland, et område eller en specifik sektor i et tredjeland, eller en international organisation har et tilstrækkeligt databeskyttelsesniveau, og dermed skabe retssikkerhed og ensartethed i hele Unionen hvad angår det tredjeland eller den internationale organisation, der vurderes at have et sådant beskyttelsesniveau. Det fremgår endvidere, at personoplysninger, i sådanne tilfælde, kan overføres til det pågældende tredjeland uden yderligere godkendelse. Endelig fremgår det, at EU-Kommissionen også kan træffe afgørelse om at tilbagekalde en sådan afgørelse efter at have underrettet og fyldestgørende begrundet det over for det pågældende tredjeland eller den pågældende internationale organisation.

Med databeskyttelsesforordningens artikel 45, stk. 1, sker der en ordlydsmæssig udvidelse i forhold til gældende ret efter persondatalovens § 27, stk. 1, idet det ikke længere kun er tredjelande, der kan konstateres som havende et tilstrækkeligt beskyttelsesniveau, men også internationale organisationer og et område eller en eller flere specifikke sektorer i tredjelandet eller den internationale organisation.

For så vidt angår områder eller en eller flere specifikke sektorer *i et tredjeland* er der imidlertid tale om en videreførelse af gældende ret, da man allerede i dag – i både teori og praksis (sektorer) – har accepteret, at disse kan sikre et tilstrækkeligt beskyttelsesniveau.

Nyt er det derimod, at internationale organisationer eller en eller flere specifikke sektorer *i en international organisation* kan sikre et tilstrækkeligt beskyttelsesniveau. Der gives ikke i databeskyttelsesforordningen eksempler på, hvilke typer internationale organisationer, der er tale om, men der er formentlig tænkt på organisationer som FN med tilhørende underorganisationer som f.eks. UNICEF eller UNHCR, Røde Kors, WHO og OECD m.fl.

Det er endvidere nyt, når det fremgår af artikel 45, stk. 1, at overførsel til et tredjeland kan finde sted, hvis *EU-Kommissionen* har fastslået, at det pågældende tredjeland m.fl. sikrer et tilstrækkeligt beskyttelsesniveau. Den mulighed for, at en dataansvarlig selv kan foretage

en vurdering af, om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau bortfalder derfor med forordningen. Den praktiske betydning heraf vil dog nok være begrænset, da det som nævnt formentlig er sjældent, at en dataansvarlig selv foretager vurderingen i praksis.

Herudover er det nyt, når det fremgår af artikel 45, stk. 1, at overførsler til tredjelande m.fl. ikke kræver specifik godkendelse. De beskrevne krav om forudgående udtalelse efter persondatalovens § 45, stk. 1, nr. 1, og forudgående tilladelse efter persondatalovens § 50, stk. 2, bortfalder således også med forordningen.

6.2.3.2. Databeskyttelsesforordningens artikel 45, stk. 2

Af databeskyttelsesforordningens artikel 45, stk. 2, fremgår det, at EU-Kommissionen ved vurderingen af et beskyttelsesniveaus tilstrækkelighed navnlig tager følgende elementer i betragtning:

a) retsstatsprincippet, respekt for menneskerettighederne og de grundlæggende frihedsrettigheder, relevant lovgivning, både generel og sektorbestemt, herunder vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og strafferet og offentlige myndigheders adgang til personoplysninger, samt gennemførelsen af sådan lovgivning, databeskyttelsesregler, faglige regler og sikkerhedsforanstaltninger, herunder regler for videreoverførsel af personoplysninger til et andet tredjeland eller en anden international organisation, der gælder i dette land eller denne internationale organisation, retspraksis samt effektive rettigheder for registrerede, som kan håndhæves, og effektiv administrativ og retslig prøvelse for de registrerede, hvis personoplysninger overføres

b) tilstedeværelse af en eller flere velfungerende uafhængige tilsynsmyndigheder i tredjelandet, eller som den internationale organisation er underlagt, med ansvar for at sikre og håndhæve, at databeskyttelsesreglerne overholdes, herunder tilstrækkelige håndhævelsesbeføjelser, for at bistå og rådgive de registrerede, når de udøver deres rettigheder, og for samarbejde med tilsynsmyndighederne i medlemsstaterne, og

c) de internationale forpligtelser, som tredjelandet eller den internationale organisation har påtaget sig, eller andre forpligtelser, der følger af retligt bindende konventioner eller instrumenter og af landets eller organisationens deltagelse i multilaterale eller regionale systemer, navnlig vedrørende beskyttelse af personoplysninger.

Det fremgår af præambelbetragtning nr. 104, at Kommissionen, i overensstemmelse med de grundlæggende værdier, som Unionen bygger på, navnlig beskyttelse af menneskerettighederne, i sin vurdering af et tredjeland eller et område eller en specifik sektor i et tredjeland bør tage hensyn til, hvordan et bestemt tredjeland efterlever retsstatsprincippet, kla-

geadgang og domstolsprøvelse, internationale menneskerettighedsnormer og -standarder samt sin generelle og sektorbestemte ret, herunder lovgivning vedrørende offentlig sikkerhed, forsvar, statens sikkerhed samt offentlig orden og strafferet. Endvidere fremgår det, at der, når der vedtages en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i et område eller en specifik sektor i et tredjeland, bør tages hensyn til klare og objektive kriterier, som f.eks. specifikke behandlingsaktiviteter og anvendelsesområdet for gældende retsstandarder og lovgivning i tredjelandet. Om beskyttelsesniveauet fremgår det endvidere, at tredjelandet bør give garantier, der sikrer et passende beskyttelsesniveau, *som i det væsentlige svarer til det, der sikres i Unionen*, især når personoplysninger behandles i en eller flere specifikke sektorer. Endelig fremgår det om tilsyn, samarbejde og rettigheder, at tredjelandet navnlig bør sikre et effektivt uafhængigt databeskyttelsestilsyn og bør fastlægge samarbejdsmekanismer med medlemsstaternes databeskyttelsesmyndigheder, og at de registrerede bør have effektive rettigheder, som kan håndhæves, og adgang til effektiv administrativ og retslig prøvelse.

Herudover fremgår det af præambelbetragtning nr. 105, at Kommissionen, ud over de internationale forpligtelser, som tredjelandet eller den internationale organisation har indgået, bør tage hensyn til forpligtelser, der følger af tredjelandets eller den internationale organisations deltagelse i multilaterale eller regionale systemer, navnlig i forbindelse med beskyttelse af personoplysninger, samt gennemførelsen af sådanne forpligtelser. I den forbindelse påpeges det, at der navnlig bør tages hensyn til tredjelandets tiltrædelse af Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger og tillægsprotokollen hertil. Endelig fremgår det, at Kommissionen bør høre Databeskyttelsesrådet, når den vurderer beskyttelsesniveauet i tredjelande eller internationale organisationer.

Ved en sammenholdelse af persondatalovens § 27, stk. 2 (direktivets artikel 25, stk. 2), og databeskyttelsesforordningens artikel 45, stk. 2, fremgår det, at forordningen oplister langt flere elementer, der skal indgå i en tilstrækkelighedsvurdering.

Mange af de yderligere elementer fremgår imidlertid også af Artikel 29-gruppens udtalelse fra 1998 (WP 12).

For så vidt angår de elementer, der både fremgår af databeskyttelsesforordningens artikel 45, stk. 2, og Artikel 29-gruppens udtalelse, vil der formentlig være tale om en videreførelse af gældende ret, selvom elementerne nu er blevet flyttet fra en Artikel 29-gruppe udtalelse og over i selve forordningsteksten.

Enkelte af elementerne i databeskyttelsesforordningens artikel 45, stk. 2, er dog blevet væsentligt præciseret, herunder f.eks. elementerne i artikel 45, stk. 2, litra a, om, at der skal ses på lovgivning om offentlige myndigheders adgang til personoplysninger mv. Disse præciserede elementer synes indsat som en konsekvens af føromtalte Schrems-sag (C-362/14), der bl.a. omhandlede amerikanske myndigheders mulighed for at masseindsamle overførte personoplysninger om europæere af hensyn til offentlig sikkerhed mv.

I forhold til de elementer, der er blevet præciseret i databeskyttelsesforordningens artikel 45, stk. 1, vil der formentlig også i vidt omfang være tale om en videreførelse af gældende ret efter dommen i Schrems-sagen.

6.2.3.3. Databeskyttelsesforordningens artikel 45, stk. 3

Det fremgår af databeskyttelsesforordningens artikel 45, stk. 3, at Kommissionen efter en vurdering af beskyttelsesniveauets tilstrækkelighed, ved hjælp af en gennemførelsesretsakt, kan fastslå, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland, eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2.

Om revision af gennemførelsesretsakten fremgår det endvidere, at der i den pågældende gennemførelsesretsakt skal fastsættes en mekanisme for regelmæssig revision, som foretages mindst hvert fjerde år, og som inddrager enhver relevant udvikling i tredjelandet eller den internationale organisation. Herudover fremgår det, at der i gennemførelsesretsakten skal angives dennes territoriale og sektorbestemte anvendelsesområde og i påkommende tilfælde den eller de tilsynsmyndigheder, der er omhandlet i denne artikels stk. 2, litra b). Endelig fremgår det, at gennemførelsesretsakten skal vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

Af 2. og 3. punktum i præambelbetragtning nr. 106, fremgår det om regelmæssig revision, at Kommissionen, i sine afgørelser om tilstrækkeligheden af beskyttelsesniveauet, bør fastsætte en mekanisme for regelmæssig revision af afgørelsernes virkning. Det fremgår endvidere, at denne regelmæssige revision bør foretages i samråd med det pågældende tredjeland eller den pågældende internationale organisation og tage hensyn til enhver relevant udvikling i tredjelandet eller den internationale organisation.

Det fremgår endvidere af 4. og 5. punktum i præambelbetragtning nr. 106, at Kommissionen, i forbindelse med overvågning og den regelmæssige revision, bør tage hensyn til synspunkter og resultater fra Europa-Parlamentet og fra Rådet såvel som fra andre relevante organer og kilder. Endvidere fremgår det, at Kommissionen inden for en rimelig frist bør evaluere virkningen af sidstnævnte afgørelser og rapportere alle relevante resultater til det

udvalg som er omhandlet i Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 (1), der nedsættes ved nærværende forordning, og til Europa-Parlamentet og Rådet.

I lighed med i gældende ret kan Kommissionen med databeskyttelsesforordningens artikel 45, stk. 3, fastslå, at et tredjeland (og nu også internationale organisationer m.fl.) sikrer et tilstrækkeligt beskyttelsesniveau.

Nyt er det, at det fremgår udtrykkeligt af bestemmelsen, at der i gennemførelsesretsakten (tilstrækkelighedsafgørelsen) skal fastsættes en mekanisme for regelmæssig revision, som skal foretages mindst hvert fjerde år.

Kravet om fastsættelse af en mekanisme for regelmæssig revision er formentlig ligeledes en konsekvens af Schrems-sagen (C-362/14), idet EU-Domstolen i sin dom understregede, at der skal ske regelmæssig revision.

Med sin tilstrækkelighedsafgørelse i forhold til EU-U.S. Privacy Shield er Kommissionen allerede i praksis begyndt at indsætte mekanismer om regelmæssig revision. Det nye krav er derfor formentlig en videreførelse af gældende ret efter dommen i Schrems-sagen (C-362/14).

En konsekvens af kravet om en mekanisme om regelmæssig revision kan være, at dataeksportører vil have mindre tillid til en tilstrækkelighedsafgørelse som overførselsgrundlag, da der kan være en potentiel fare for, at en revision fører til suspension eller ophævelse. En tilstrækkelighedsafgørelse kan således risikere at blive betragtet som en kortsigtet løsning for dataeksportørerne.

Kravet om, at der i en tilstrækkelighedsafgørelse skal angives de relevante tilsynsmyndigheder i tredjelandet m.fl. er nyt i forhold til gældende ret. I praksis angives de relevante tilsynsmyndigheder somme tider i de dokumenter, der ligger til grund for en tilstrækkelighedsafgørelse.[690]

6.2.3.4. Databeskyttelsesforordningens artikel 45, stk. 4

Af databeskyttelsesforordningens artikel 45, stk. 4, fremgår det, at Kommissionen løbende skal overvåge udviklingen i tredjelande og internationale organisationer, der kan påvirke virkningen af afgørelser, der er vedtaget i henhold til denne artikels stk. 3, og afgørelser og beslutninger, der er vedtaget på grundlag af artikel 25, stk. 6, i databeskyttelsesdirektivet.

[690] Se f.eks. aftalegrundlaget for EU-U.S. Privacy Shield her (de syv annekser).

Om løbende overvågning af udviklingen fremgår det tilsvarende af præambelbetragtning nr. 106, 1. punktum, at Kommissionen bør overvåge virkningen af afgørelser om beskyttelsesniveauet i et tredjeland, et område eller en specifik sektor i et tredjeland, eller en international organisation, og overvåge virkningen af afgørelser vedtaget på grundlag af artikel 25, stk. 6, eller artikel 26, stk. 4, i databeskyttelsesdirektivet.

Der henvises endelig til gennemgangen af præambelbetragtning nr. 106, 4. og 5. punktum ovenfor.

Databeskyttelsesforordningens artikel 45, stk. 4, må antages at være en videreførelse af den praksis, som Kommissionen – i lyset af Schrems-sagen (C-362/14) – har anlagt i forhold til EU-U.S. Privacy Shield.

6.2.3.5. Databeskyttelsesforordningens artikel 45, stk. 5

Af databeskyttelsesforordningens artikel 45, stk. 5, fremgår det, at Kommissionen, i det omfang, det er nødvendigt, uden tilbagevirkende kraft, skal ophæve, ændre eller suspendere en afgørelse omhandlet af artikel 45, stk. 3, ved hjælp af gennemførelsesretsakter, hvis tilgængelige oplysninger, navnlig efter den i artikel 45, stk. 3 omhandlede revision, viser, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland, eller en international organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 45, stk. 2. Endvidere fremgår det, at disse gennemførelsesretsakter skal vedtages efter undersøgelsesproceduren i artikel 93, stk. 2. Dog fremgår det tillige, at Kommissionen, i behørigt begrundede særligt hastende tilfælde, efter proceduren i artikel 93, stk. 3, kan vedtage gennemførelsesretsakter, der finder anvendelse straks.

Endvidere fremgår det af præambelbetragtning nr. 107, 1. punktum, at Kommissionen kan fastslå, at et tredjeland, et område eller en specifik sektor i et tredjeland, eller en international organisation ikke længere sikrer et tilstrækkeligt databeskyttelsesniveau.

Artikel 45, stk. 5, må antages at være en videreførelse af gældende ret.

6.2.3.6. Databeskyttelsesforordningens artikel 45, stk. 6

Det fremgår af databeskyttelsesforordningens artikel 45, stk. 6, at Kommissionen skal føre konsultationer med tredjelandet eller den internationale organisation med henblik på at afhjælpe den situation, der har givet anledning til en afgørelse vedtaget i henhold til stk. 5.

Af 3. og 4. punktum i præambelbetragtning nr. 107, fremgår det om afhjælpning, at der i sådanne tilfælde bør fastlægges bestemmelser om en procedure for konsultationer mellem Kommissionen og sådanne tredjelande eller internationale organisationer. Endvidere frem-

går det, at Kommissionen rettidigt bør underrette tredjelandet eller den internationale organisation om årsagerne og indlede konsultationer med tredjelandet eller den internationale organisation for at afhjælpe situationen.

Det må antages, at artikel 45, stk. 6, ligeledes er en videreførelse af gældende ret.

6.2.3.7. Databeskyttelsesforordningens artikel 45, stk. 7

Af databeskyttelsesforordningens artikel 45, stk. 7, fremgår det, at en afgørelse efter artikel 45, stk. 5, ikke berører en overførsel af personoplysninger til det pågældende tredjeland, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation i medfør af artikel 46-49.

Om brug af de andre overførselsgrundlag i forbindelse med en afgørelse efter § 45, stk. 5, fremgår det af præambelbetragtning nr. 107, 2. punktum, at overførsel af personoplysninger til et sådant tredjeland eller en sådan international organisation bør forbydes, medmindre kravene i databeskyttelsesforordningen vedrørende overførsel omfattet af fornødne garantier, herunder bindende virksomhedsregler og undtagelser i særlige situationer, er opfyldt.

Artikel 45, stk. 7, må antages at være en videreførelse af gældende ret.

6.2.3.8. Databeskyttelsesforordningens artikel 45, stk. 8

Det fremgår af databeskyttelsesforordningens artikel 45, stk. 8, at Kommissionen, i *Den Europæiske Unions Tidende* og på sit websted, offentliggør en liste over tredjelande, områder og specifikke sektorer i tredjelande samt internationale organisationer, som den har fastslået sikrer eller ikke længere sikrer et tilstrækkeligt beskyttelsesniveau.

Selvom det er nyt, at det nu fremgår udtrykkeligt af artikel 45, stk. 8, at en tilstrækkelighedsafgørelse skal offentliggøres i Den Europæiske Unions Tidende og på Kommissionens hjemmeside, er der i praksis tale om en videreførelse af gældende ret.

6.2.3.9. Databeskyttelsesforordningens artikel 45, stk. 9

Af databeskyttelsesforordningens artikel 45, stk. 9, fremgår det, at afgørelser og beslutninger, der er vedtaget af Kommissionen på grundlag af artikel 25, stk. 6, i databeskyttelsesdirektivet, fortsat gælder, indtil de ændres, erstattes eller ophæves ved en kommissionsafgørelse, der vedtages i henhold til nærværende artikel 45, stk. 3 eller 5.

For en oversigt over de tredjelande, hvor Kommissionen på nuværende tidspunkt på grundlag af artikel 25, stk. 6, i databeskyttelsesdirektivet har truffet afgørelse om, at de pågældende lande sikrer et tilstrækkeligt beskyttelsesniveau henvises til afsnit 6.2.2.3.

6.2.4. Overvejelser

Databeskyttelsesforordningens artikel 45 er i vidt omfang en videreførelse af gældende ret.

I forhold til forordningens artikel 45, stk. 1, er det dog nyt, at internationale organisationer eller en eller flere specifikke sektorer i en international organisation kan sikre et tilstrækkeligt beskyttelsesniveau.

Det er endvidere nyt, at det efter artikel 45, stk. 1, alene er Kommissionen, der kan fastslå, at et tredjeland m.fl. sikrer et tilstrækkeligt beskyttelsesniveau. Efter de gældende regler har de dataansvarlige også selv mulighed for at foretage vurderingen, idet det dog må antages sjældent at være sket i praksis.

Herudover er det nyt, når det fremgår af artikel 45, stk. 1, at overførsler til tredjelande m.fl. ikke kræver specifik godkendelse. De beskrevne krav om forudgående udtalelse efter persondatalovens § 45, stk. 1, nr. 1, og forudgående tilladelse efter persondatalovens § 50, stk. 2, bortfalder således også med forordningen.

Kravet i forordningens artikel 45, stk. 3, om at der i en tilstrækkelighedsafgørelse skal angives de relevante tilsynsmyndigheder i tredjelandet m.fl. er nyt i forhold til gældende ret. I praksis angives de relevante tilsynsmyndigheder dog somme tider i de dokumenter, der ligger til grund for en tilstrækkelighedsafgørelse.

6.3. Overførsler omfattet af fornødne garantier, artikel 46

6.3.1. Præsentation

I databeskyttelsesforordningens artikel 46 fastsættes der regler for, hvornår en dataansvarlig eller en databehandler – ved at give tilstrækkelige garantier – må overføre personoplysninger til et tredjeland, som Kommissionen ikke i medfør af artikel 45, stk. 3, har fastslået sikrer et tilstrækkeligt beskyttelsesniveau.

Nogle af reglerne i artikel 46 er umiddelbart kendt fra databeskyttelsesdirektivet og persondataloven, mens andre er helt nye.

6.3.2. Gældende ret

6.3.2.1. Persondatalovens § 27, stk. 4

Det fremgår af persondatalovens § 27, stk. 4, at tilsynsmyndigheden (Datatilsynet) uden for de i stk. 3 (undtagelser i særlige situationer) nævnte tilfælde kan give tilladelse til, at der overføres oplysninger til tredjelande, som ikke opfylder stk. 1 (lande som sikrer et tilstrækkeligt beskyttelsesniveau), såfremt den dataansvarlige yder tilstrækkelige garantier for beskyttelse af den registreredes rettigheder. Herudover fremgår det af bestemmelsen, at der kan fastsættes nærmere vilkår for overførslen. Endelig fremgår det, at Datatilsynet skal underrette Kommissionen og de øvrige medlemsstater om tilladelser meddelt i henhold til bestemmelsen.

Af bemærkningerne til persondataloven fremgår det bl.a. om de tilstrækkelige garantier, at disse skal ydes for beskyttelsen af privatlivets fred, personers grundlæggende rettigheder og frihedsrettigheder samt for udøvelsen af de dertil knyttede rettigheder.[691] Det fremgår endvidere af bemærkningerne, at garantierne navnlig kan fremgå af passende kontraktbestemmelser, som medfører, at det beskyttelsesniveau, som loven tilsigter at sikre, ikke forringes væsentligt.

Når ordlyden af persondatalovens § 27, stk. 4, og ovennævnte bemærkninger til loven sammenholdes, dækker de stort set indholdet af databeskyttelsesdirektivets artikel 26, stk. 2 og 3[692], som persondatalovens § 27, stk. 4, har sin baggrund i.

6.3.2.1.1. Kommissionens standardkontraktbestemmelser

Kommissionen har i medfør af databeskyttelsesdirektivets artikel 26, stk. 4 – efter proceduren i direktivets artikel 31, stk. 2 – fastslået, at visse standardkontraktbestemmelser indeholder tilstrækkelige garantier for privatlivets fred, personers grundlæggende rettigheder og frihedsrettigheder samt for udøvelsen af de dertil knyttede rettigheder.

Kontrakter, der udarbejdes i overensstemmelse med Kommissionens standardkontraktbestemmelser, vil således automatisk opfylde kravet i persondatalovens § 27, stk. 4.

Der findes pt. to sæt standardkontraktbestemmelser vedrørende overførsel af oplysninger fra en *dataansvarlig i EU til en dataansvarlig i et tredjeland*[693] og et sæt standardkontrakt-

[691] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 27, stk. 4.
[692] Se også Databeskyttelsesdirektivets præambelbetragtning 59.
[693] Kommissionens beslutning af 15. juni 2001 (2001/497/EF) og Kommissionens beslutning af 27. december 2004 (2004/915/EF).

bestemmelser vedrørende overførsel af oplysninger fra en *dataansvarlig i EU til en databehandler i et tredjeland.*[694]

Om de tilfælde, hvor Kommissionen ikke har fastsat standardkontraktbestemmelser fremgår det af Registerudvalgets betænkning nr. 1345,[695] at tilsynsmyndigheden selv må foretage en vurdering af, om den pågældende aftale eller andre foranstaltninger, som den dataansvarlige iværksætter, kan antages at sikre, at der ikke sker en væsentlig forringelse af den beskyttelse, som lovudkastet tilsigter at sikre.

Ovennævnte vil i praksis også gøre sig gældende i de situationer, hvor Kommissionen har fastsat standardkontraktbestemmelser, men hvor en dataansvarlig ikke ønsker at benytte disse, eller hvor en dataansvarlig ønsker at benytte standardkontraktbestemmelserne med ændringer.

Kontrakter, der afviger fra Kommissionens standardkontraktbestemmelser, betegnes i daglig tale som ad hoc kontrakter.

Se mere om Kommissionens standardkontraktbestemmelser og ad hoc kontrakter nedenfor. Se også Kommissionens FAQ vedrørende overførsel af personoplysninger til tredjelande, som kan findes på Kommissionens hjemmeside for databeskyttelse.

6.3.2.1.2. Underretning af Kommissionen og de øvrige medlemsstater om tilladelser efter § 27, stk. 4

Efter persondatalovens § 27, stk. 4, sidste punktum, skal tilsynsmyndigheden underrette Kommissionen og de øvrige medlemsstater om tilladelser meddelt i henhold til bestemmelsen. I praksis skal sådanne underretninger dog kun gives, hvis der meddeles tilladelse til en overførsel baseret på en ad hoc kontrakt.

Hvis berettigelsen af en tilladelse – i forbindelse med en underretning – drages i tvivl af en medlemsstat eller Kommissionen, kan Kommissionen i medfør af databeskyttelsesdirektivets artikel 26, stk. 3, 2. led, vedtage passende foranstaltninger efter proceduren i artikel 31, stk. 2. Vedkommende tilsynsmyndighed skal i så fald træffe de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse.

[694] Kommissionens afgørelse af 5. februar 2010 (K (2010) 593 endelig.
[695] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 289.

I Danmark kunne en sådan foranstaltning bestå i, at Datatilsynet måtte tilbagekalde en tilladelse meddelt efter persondatalovens § 27, stk. 4, jf. lovens § 58, stk. 2.[696] Dette er endnu ikke sket i praksis.

6.3.2.2. Overførsler efter persondatalovens § 27, stk. 4, der ikke kræver tilladelse fra Datatilsynet

Indtil 1. januar 2013 krævede alle overførsler til tredjelande baseret på persondatalovens § 27, stk. 4, tilladelse fra Datatilsynet.

Langt hovedparten af de tilladelser, der blev givet før den 1. januar 2013 vedrørte imidlertid anmodninger om overførsel af oplysninger til tredjelande baseret på Kommissionens standardkontraktbestemmelser, og antallet af anmodninger var stigende.[697]

På denne baggrund blev der indsat et nyt stk. 5 i persondatalovens § 27, hvorefter overførsel af oplysninger til tredjelande kan ske uden tilladelse efter § 27, stk. 4, på grundlag af kontrakter, der er i overensstemmelse med standardkontraktbestemmelser, som er godkendt af Kommissionen.[698]

Overførsler til tredjelande baseret på en af Kommissionens tre standardkontraktbestemmelser kræver således ikke længere tilladelse fra Datatilsynet.

Det er i den forbindelse vigtigt at være opmærksom på, at det fremgår af ordlyden til § 27, stk. 5, at bestemmelsen kun finder anvendelse, hvis den anvendte kontrakt er *i overensstemmelse* med Kommissionens standardkontraktbestemmelser. Hvis der foretages ændringer i forhold til Kommissionens standardkontraktbestemmelser, skal der fortsat indhentes tilladelse fra Datatilsynet.

I Datatilsynets praksis[699] betragtes selv små sproglige ændringer, af Kommissionens standardkontraktbestemmelser, som ændringer, der medfører, at § 27, stk. 5, ikke finder anvendelse.

Ved brug af Kommissionens standardkontraktbestemmelser er det i øvrigt vigtigt, at den dataansvarlige (dataeksportøren) sætter sig grundigt ind i kontraktens indhold, så den dataansvarlige er sikker på, at alle kontraktens parter kan leve op til deres forpligtelser. I Kommissionens standardkontraktbestemmelser fra 2010, vedrørende overførsel fra en da-

[696] Persondataloven med kommentarer (2015), s. 456.
[697] Forslag nr. L 15 fremsat den 3. oktober 2012 om bl.a. ændring af lov om personoplysninger, afsnit 2.1.2.
[698] Se lov nr. 1245 af 18. december 2012.
[699] F.eks. Datatilsynets j.nr. 2012-233-0143.

taansvarlig til en databehandler, er der f.eks. i standardbestemmelse 4, litra f, en særlig bestemmelse om oplysningspligt ved overførsel af følsomme personoplysninger. Herudover skal standardkontraktbestemmelserne udfyldes af parterne.

6.3.2.3. Overførsler efter persondatalovens § 27, stk. 4, der kræver tilladelse fra Datatilsynet

6.3.2.3.1. Bindende virksomhedsregler

Størstedelen af de tilladelser, der i dag meddeles efter persondatalovens § 27, stk. 4, er tilladelser til at overføre oplysninger til tredjelande baseret på et godkendt sæt bindende virksomhedsregler. Bindende virksomhedsregler behandles særskilt i afsnit 6.4., hvorfor disse ikke vil blive omtalt yderligere i dette afsnit.

6.3.2.3.2. Ad hoc kontrakter

Datatilsynets tilladelser efter § 27, stk. 4, vedrører i øvrigt de såkaldte ad hoc kontrakter – dvs. kontrakter, der ikke er i overensstemmelse med Kommissionens standardkontraktbestemmelser, herunder fordi der er foretaget ændringer.

Datatilsynet modtager ikke mange anmodninger om tilladelse til, efter persondatalovens § 27, stk. 4, at overføre personoplysninger til tredjelande baseret på ad hoc kontrakter.

I praksis kan de få ad hoc kontrakter, som Datatilsynet modtager til godkendelse, typisk inddeles i to kategorier.

Den første kategori er kontrakter, hvori der er foretaget ændringer i Kommissionens standardkontraktbestemmelser. Ændringerne kan bestå i alt fra mindre sproglige rettelser til større indholdsmæssige ændringer, hvor f.eks. kontrakternes bestemmelser om tredjepartsløfter eller dataimportørens forpligtelser ønskes begrænset.

Hvis Datatilsynets tilladelse ønskes i forhold til denne type kontrakter, kræver dette i praksis, at den dataansvarlige oplyser tilsynet om, hvilke rettelser der er foretaget i standardkontraktbestemmelserne, samt fyldestgørende redegør for ændringernes betydning i forhold til de tilstrækkelige garantier, der skal ydes med hensyn til de registreredes rettigheder.

Kan en dataansvarlig i den forbindelse sandsynliggøre, at en ændring, i forhold til Kommissionens standardkontraktbestemmelser, ikke vil føre til en ringere retsstilling for de registrerede, vil Datatilsynet normalt meddelelse tilladelse efter § 27, stk. 4.[700]

Som eksempler på ændringer, der typisk godt vil kunne accepteres kan nævnes 1) mindre sproglige ændringer hvor f.eks. "dataeksportør" og "dataimportør" udskiftes med kontraktparternes navne og 2) indsættelse af supplerende kommercielle bestemmelser, hvis disse hverken direkte eller indirekte har betydning for det materielle indhold af standardbestemmelserne.

Den anden kategori er kontrakter, hvor (oftest) en virksomhed ønsker at indsætte flere dataeksportører og/eller dataimportører i samme kontrakt. Disse kontrakter kan især være hensigtsmæssige, hvis der sker mange ensartede overførsler til tredjelande.[701]

Ønskes Datatilsynets tilladelse til overførsel af oplysninger, baseret på en standardkontraktbestemmelse indeholdende flere dataeksportører og/eller dataimportører, kræver dette i praksis, at der er vedlagt lister med navnene på alle kontraktparterne, ligesom der skal være de fornødne underskrifter fra de tegningsberettigede personer.[702]

Herudover er det normalt en forudsætning for at opnå Datatilsynets tilladelse, at alle kontraktparterne skal overføre oplysninger med de samme formål, og at alle kontraktparterne overfører de samme oplysningstyper. Dette skyldes, at bilagene til standardkontraktbestemmelserne – efter Datatilsynets opfattelse – ellers ikke vil kunne udfyldes meningsfuldt. Dette vil kunne skabe manglende overblik blandt kontraktparterne, hvilket kan føre til, at der i praksis ikke kan ydes tilstrækkelige garantier for de registreredes rettigheder.

Datatilsynet har de seneste år modtaget færre anmodninger om tilladelse til at overføre oplysninger til tredjelande baseret på ad hoc kontrakter med flere dataeksportører og/eller dataimportører. Dette skyldes formentlig en øget brug af bindende virksomhedsregler, som siden 1. januar 2013 også har været muligt for koncerner, der alene virker som databehandlere.[703]

---

[700] I Datatilsynets sag med j.nr. 2013-233-0175 kunne det ikke sandsynliggøres, at en ændring ikke ville føre til en ringere retsstilling for de registrerede.
[701] Der er f.eks. givet tilladelser i Datatilsynets sager med j.nr. 2007-233-0087 og 2008-233-0118.
[702] Se f.eks. Datatilsynets sag med j.nr. 2012-233-0036.
[703] Se Artikel 29-gruppens udtalelse af 6. juni 2012 om bindende virksomhedsregler for databehandlere (WP 195).

6.3.2.3.3. Artikel 29- gruppens udtalelse om de indholdsmæssige krav til en kontrakt
Artikel 29-gruppen har i en udtalelse af 24. juli 1998 om overførsel af personoplysninger til tredjelande (WP 12) bl.a. udtalt sig om brugen af kontrakter som overførselsgrundlag. På side 16 ff. i udtalelsen opstiller Artikel 29-gruppen en række specifikke krav til en kontraktløsning.

Ifølge Artikel 29-gruppen skal en kontrakt – for at kunne yde tilstrækkelige garantier – som minimum indeholde grundlæggende principper som 1) formålsafgrænsning, 2) datakvalitet- og dataproportionalitet, 3) gennemsigtighed, 4) sikkerhed, 5) ret til indsigt, berigtigelse og indsigelse samt 6) begrænsninger i videreoverførsler. Herudover udtaler Artikel 29-gruppen, at der i visse situationer gælder yderligere principper vedrørende følsomme oplysninger, direkte markedsføring og edb-baserede afgørelser.

Artikel 29-gruppen udtaler endvidere, at en kontrakt skal indeholde midler til at håndhæve ovennævnte principper, herunder f.eks. i form af bestemmelser om støtte og hjælp til individuelle registrerede med at udøve deres rettigheder og bestemmelser om passende genoprejsning til skadelidte i tilfælde af, at reglerne overtrædes.

Hvis en dataansvarlig ønsker at benytte en kontrakt, som den dataansvarlige selv har konciperet, bør den dataansvarlige således sikre sig, at, som minimum, alle principperne mv. fra Artikel 29-gruppens udtalelse er indeholdt i kontrakten. I modsat fald kan den dataansvarlige ikke forvente at blive meddelt tilladelse efter persondatalovens § 27, stk. 4.

Generelt kan det dog anbefales at benytte – eller som minimum tage udgangspunkt i – Kommissionens standardkontraktbestemmelser, da disse som udgangspunkt altid sikrer et tilstrækkeligt beskyttelsesniveau. Standardkontraktbestemmelserne er også kendt af tilsynsmyndighederne, hvorfor sagsbehandlingen typisk vil være væsentlig kortere, når disse benyttes.

6.3.2.3.4. Samarbejdsprocedure for standardkontraktbestemmelser
Organisationer (typisk virksomheder), der opererer i flere medlemsstater, og som ønsker at benytte ad hoc kontrakter som overførselsgrundlag, kan med fordel overveje at benytte den samarbejdsprocedure, der er fastsat i Artikel 29-gruppens udtalelse af 26. november 2014[704] om en samarbejdsprocedure vedrørende standardkontraktbestemmelser.

I udtalelsen fra Artikel 29-gruppen fastsættes der en procedure, hvorefter en virksomhed, der ønsker at få godkendt en ad hoc kontrakt (standardkontraktbestemmelse med ændrin-

[704] Artikel 29-gruppens Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" Considered as compliant with the EC Model Clauses (WP 226).

ger) i flere medlemsstater, kan nøjes med at gå til en "ledende tilsynsmyndighed". Denne ledende tilsynsmyndighed vil herefter, når den er tilfreds med indholdet af ad hoc kontrakten, sende et udkast til et brev til de relevante tilsynsmyndigheder, der bekræfter, at kontrakten yder tilstrækkelige garantier for de registreredes rettigheder.

De medlemsstater, der har tilsluttet sig samarbejdsproceduren, vil herefter lægge den ledende tilsynsmyndigheds vurdering til grund, når de bliver anmodet om tilladelse til at overføre oplysninger til tredjelande baseret på den pågældende kontrakt. Det skal bemærkes, at det varierer fra medlemsstat til medlemsstat, i hvilket omfang der skal meddeles tilladelse til at overføre oplysninger til tredjelande.

I Danmark deltager Datatilsynet ikke i ovennævnte samarbejdsprocedure, idet en deltagelse heri – efter tilsynets opfattelse – ikke vil være foreneligt med persondatalovens § 27, stk. 4, samt det forvaltningsretlige officialprincip. Tilsynet vil dog normalt tillægge det vægt, hvad en anden tilsynsmyndighed måtte have konkluderet i forhold til en given ad hoc kontrakt.

6.3.3. Databeskyttelsesforordningen

6.3.3.1. Databeskyttelsesforordningens artikel 46, stk. 1

Af databeskyttelsesforordningens artikel 46, stk. 1, fremgår det, at hvis der ikke er vedtaget en afgørelse i henhold til artikel 45, stk. 3, må en dataansvarlig eller databehandler kun overføre personoplysninger til et tredjeland eller en international organisation, hvis vedkommende har givet de fornødne garantier, og på betingelse af at rettigheder, som kan håndhæves, og effektive retsmidler for registrerede er tilgængelige.

Det fremgår i lighed hermed af præambelbetragtning nr. 108, at den dataansvarlige eller databehandleren, i mangel af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, bør træffe foranstaltninger for at kompensere for den manglende databeskyttelse i et tredjeland i form af fornødne garantier for den registrerede.

Ifølge præambelbetragtning nr. 108 kan fornødne garantier bestå i anvendelse af bindende virksomhedsregler, standardbestemmelser om databeskyttelse vedtaget af Kommissionen, standardbestemmelser om databeskyttelse vedtaget af en tilsynsmyndighed eller kontraktbestemmelser godkendt af en tilsynsmyndighed, jf. artikel 46, stk. 2 og 3.

Formålet med de fornødne garantier er, ifølge præambelbetragtning nr. 108, at sikre overholdelse af databeskyttelseskravene og de registreredes rettigheder i forbindelse med intern behandling i Unionen, herunder tilgængelighed af rettigheder, som kan håndhæves, for

registrerede og effektive retsmidler, herunder til at opnå effektiv administrativ eller retslig prøvelse og til at kræve erstatning, i Unionen eller et tredjeland.

Herudover fremgår det af præambelbetragtning nr. 108, at garantierne navnlig bør vedrøre overholdelse af de generelle principper for behandling af personoplysninger og principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

Af præambelbetragtning nr. 114 fremgår det endvidere, at hvis Kommissionen ikke har truffet afgørelse om tilstrækkeligheden af databeskyttelsesniveauet i et tredjeland, bør den dataansvarlige eller databehandleren under alle omstændigheder benytte løsninger, der giver de registrerede effektive rettigheder, som kan håndhæves, hvad angår behandlingen af deres personoplysninger i Unionen, når disse oplysninger er blevet overført, så de fortsat vil nyde godt af grundlæggende rettigheder og garantier.

Som i persondatalovens § 27, stk. 4, er udgangspunktet i databeskyttelsesforordningens artikel 46, stk. 1, at en overførsel til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau, kun må finde sted, hvis den dataansvarlige har givet de fornødne garantier for beskyttelse af de registreredes rettigheder samt for udøvelsen af disse.

Nyt er det derimod, når det fremgår af artikel 46, stk. 1, at også en databehandler skal give de fornødne garantier mv., når denne overfører personoplysninger til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau. I dag vil det altid være den dataansvarlige, der har ansvaret for at give de fornødne garantier.

Tilføjelsen af databehandlere i artikel 46, stk. 1, må antages at hænge sammen med reglen i databeskyttelsesforordningens artikel 28, stk. 4, hvorefter der åbnes op for, at en databehandler i visse situationer selv skal indgå en kontrakt eller andet retligt dokument med de underdatabehandlere, som databehandleren måtte vælge at gøre brug af.

6.3.3.2. Databeskyttelsesforordningens artikel 46, stk. 2

Det fremgår af databeskyttelsesforordningens artikel 46, stk. 2, at de fornødne garantier i stk. 1 *uden krav om specifik godkendelse fra en tilsynsmyndighed* kan sikres gennem:

> a) et retligt bindende instrument, som kan håndhæves, mellem offentlige myndigheder eller organer
>
> b) bindende virksomhedsregler i overensstemmelse med artikel 47

c) standardbestemmelser om databeskyttelse vedtaget af Kommissionen efter undersøgelsesproceduren i artikel 93, stk. 2

d) standardbestemmelser om databeskyttelse vedtaget af en tilsynsmyndighed og godkendt af Kommissionen efter undersøgelsesproceduren i artikel 93, stk. 2

e) 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, eller

f) 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.

I forhold til offentlige myndigheder fremgår det særligt af præambelbetragtning nr. 108, at overførsel kan foretages af offentlige myndigheder eller organer til offentlige myndigheder eller organer i tredjelande eller til internationale organisationer med tilsvarende opgaver eller funktioner, herunder på grundlag af bestemmelser, der medtages i administrative ordninger, f.eks. et aftalememorandum, hvorved de registrerede sikres effektive rettigheder, som kan håndhæves. Det fremgår endvidere, at en godkendelse fra den kompetente tilsynsmyndighed bør indhentes, når garantierne indgår i administrative ordninger, der ikke er juridisk bindende.

For så vidt angår muligheden for at lade standardbestemmelser være en del af en bredere kontrakt, fremgår det af præambelbetragtning nr. 109, at den dataansvarliges eller databehandlerens mulighed for at bruge standardbestemmelser om databeskyttelse vedtaget af Kommissionen eller en tilsynsmyndighed hverken bør udelukke muligheden for, at den dataansvarlige eller databehandleren medtager standardbestemmelser om databeskyttelse i en bredere kontrakt, såsom en kontrakt mellem databehandleren og en anden databehandler, eller medtager andre bestemmelser eller yderligere garantier, såfremt de hverken direkte eller indirekte er i strid med de standardkontraktbestemmelser, der er vedtaget af Kommissionen eller en tilsynsmyndighed, eller berører de registreredes grundlæggende rettigheder eller frihedsrettigheder.

Endvidere fremgår det af samme præambelbetragtning, at dataansvarlige og databehandlere bør tilskyndes til at give yderligere garantier gennem kontraktmæssige forpligtelser, der supplerer standardbestemmelserne om beskyttelse.

Ved at sammenholde forordningens artikel 46, stk. 2, med gældende ret kan det konstateres, at de garantier, der kan sikres ved hjælp af instrumenterne i litra a og d-f, er nyskabelser, hvorimod instrumenterne i litra b og c er kendte.

I forhold til de kendte instrumenter – bindende virksomhedsregler og Kommissionens standardkontraktbestemmelser – er det for så vidt angår førstnævnte nyt, at overførsler baseret på disse ikke længere kræver specifik godkendelse fra en tilsynsmyndighed (fra hver enkelt tilsynsmyndighed). Bindende virksomhedsregler skal i stedet kun godkendes af den kompetente tilsynsmyndighed efter udtalelse fra det kommende Databeskyttelsesrådsråd, jf. forordningens artikel 64, stk. 1, litra f. I forhold til Kommissionens standardkontraktbestemmelser er betragtningerne i præambelbetragtning nr. 109 i vidt omfang en videreførelse af gældende ret.

For så vidt angår de i artikel 46, stk. 2, litra a, nævnte retligt bindende instrumenter, der kan håndhæves, mellem offentlige myndigheder eller organer, fremgår det som nævnt af præambelbetragtning nr. 108, at disse f.eks. kan bestå i et aftalememorandum, hvorved de registrerede sikres effektive rettigheder, som kan håndhæves. Instrumentet i litra a kan måske i praksis tænkes anvendt i forhold til offentligretlige udvekslingsaftaler, herunder f.eks. på skatteområdet mv.

Med databeskyttelsesforordningens artikel 46, stk. 2, litra d, får tilsynsmyndighederne mulighed for at udarbejde standardkontraktbestemmelser, som, hvis de godkendes af Kommissionen efter proceduren i artikel 93, stk. 2 (inddragelse af medlemsstaterne), kan benyttes på lige fod med Kommissionens egne standardkontraktbestemmelser.

Det er meget tænkeligt, at tilsynsmyndighederne i et vist omfang vil benytte sig af bestemmelsen i litra d. Der er således allerede i dag eksempler på, at tilsynsmyndighederne har forsøgt at få Kommissionen til at vedtage standardkontraktbestemmelser. Der kan i den sammenhæng henvises til Artikel 29-gruppens udtalelse af 21. marts 2014 om et udkast til en ad hoc kontrakt vedrørende overførsel af oplysninger fra en databehandler i EU til en databehandler i et tredjeland (WP 214). Forslaget fra Artikel 29-gruppen er begrundet i, at Kommissionens egne standardkontraktbestemmelser[705] ikke giver mulighed for at anvende

[705] Se Kommissionens afgørelse af 5. februar 2010 (K (2010)593 endelig).

den foreslåede konstruktion, samt at der vedvarende har været en stor efterspørgsel fra erhvervslivet efter en løsning, som den foreslåede.

Instrumenterne i artikel 46, stk. 2, litra e og f (adfærdskodeks og certificeringer), er som nævnt også nye i forhold til gældende ret. Muligheden for at benytte adfærdskodekser og certificeringer, som grundlag for overførsel til tredjelande, må antages især at kunne blive interessant for de små og mellemstore virksomheder. Dette skyldes bl.a., at et eksisterende overførselsgrundlag som bindende virksomhedsregler primært er relevant for større koncernvirksomheder, og at standardkontraktbestemmelserne kan være svære at overskue, hvis en virksomhed ikke er i besiddelse af en juridisk afdeling eller lignende.

6.3.3.3. Databeskyttelsesforordningens artikel 46, stk. 3

Af databeskyttelsesforordningens artikel 46, stk. 3, fremgår det, at de fornødne garantier i stk. 1 – *med forbehold af godkendelse fra den kompetente tilsynsmyndighed* – også kan sikres gennem navnlig:

> a) kontraktbestemmelser mellem den dataansvarlige eller databehandleren og den dataansvarlige, databehandleren eller modtageren af personoplysninger i tredjelandet eller den internationale organisation, eller
>
> b) bestemmelser, der medtages i administrative ordninger mellem offentlige myndigheder eller organer, og som omfatter effektive rettigheder, som kan håndhæves, for registrerede.

Efter forordningens artikel 46, stk. 3, litra a, kan selvkonciperede ad hoc kontrakter benyttes som overførselsgrundlag, hvis der er indhentet en godkendelse fra den kompetente tilsynsmyndighed. Dette er en videreførelse af gældende ret. Nyt er det dog, at en ad hoc kontrakt også kan indgås mellem en databehandler og en modtager i et tredjeland. Tilføjelsen af databehandlere må, som nævnt ovenfor antages at hænge sammen med reglen i databeskyttelsesforordningens artikel 28, stk. 4, hvorefter der åbnes op for, at en databehandler i visse situationer selv skal indgå en kontrakt eller andet retligt dokument med de underdatabehandlere, som databehandleren måtte vælge at gøre brug af.

For så vidt angår instrumenterne i artikel 46, stk. 3, litra b, henvises der til ovenfor med den tilføjelse, at det kræver godkendelse fra den kompetente tilsynsmyndighed, hvis instrumentet ikke er retligt bindende.

6.3.3.4. Databeskyttelsesforordningens artikel 46, stk. 4
Det fremgår af databeskyttelsesforordningens artikel 46, stk. 4, at tilsynsmyndigheden anvender den sammenhængsmekanisme, der er omhandlet i artikel 63, i de tilfælde, der er omhandlet i artikel 46, stk. 3.

Bestemmelsen i artikel 46, stk. 4, er ny, og den er indsat for at sikre, at der sker en ensretning i forhold til, hvornår tilsynsmyndighederne godkender ad hoc kontrakter mv. Dette vil formentlig lette byrden i forhold til f.eks. virksomheder, der opererer i flere medlemsstater, da de fremadrettet må kunne gå ud fra, at svaret vil være det samme i alle medlemsstater, hvilket ikke altid er tilfældet i dag.

Det bemærkes, at det fremgår af forordningens artikel 64, stk. 1, litra e, at det kun er ved godkendelser efter artikel 46, stk. 3, litra a, at Databeskyttelsesrådet skal udtale sig, inden der sker godkendelse. Der synes således at være en diskrepans mellem ordlyden af artikel 46, stk. 4, og artikel 64, stk. 1, litra e. Det er svært at sige, hvad diskrepansen nærmere kommer til at betyde i praksis.

6.3.3.5. Databeskyttelsesforordningens artikel 46, stk. 5
Af databeskyttelsesforordningens artikel 46, stk. 5, fremgår det, at godkendelser fra en medlemsstat eller en tilsynsmyndighed på grundlag af artikel 26, stk. 2, i databeskyttelsesdirektivet er gyldige, indtil de om nødvendigt ændres, erstattes eller ophæves af den pågældende tilsynsmyndighed.

Endvidere fremgår det af bestemmelsen, at afgørelser og beslutninger, der er vedtaget af Kommissionen på grundlag af artikel 26, stk. 4, i databeskyttelsesdirektivet, er i kraft, indtil de om nødvendigt ændres, erstattes eller ophæves ved en kommissionsafgørelse, der vedtages i henhold til artikel 46, stk. 2.

6.3.4. Overvejelser
For så vidt angår databeskyttelsesforordningens artikel 46, stk. 1, er det nyt, at en databehandler også skal give de fornødne garantier mv., når denne overfører personoplysninger til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau. Tilføjelsen af *databehandlere* i artikel 46, stk. 1, må antages at hænge sammen med reglen i databeskyttelsesforordningens artikel 28, stk. 4.

I forhold til forordningens artikel 46, stk. 2, da er instrumenterne (til at sikre de fornødne garantier) i litra a og d-f, nyskabelser, hvorimod instrumenterne i litra b og c er kendte. Med hensyn til de kendte instrumenter er det – for så vidt angår bindende virksomhedsregler – nyt, at overførsler baseret på disse ikke længere kræver godkendelse fra hvert enkelt

tilsyn, men alene fra den kompetente tilsynsmyndighed efter udtalelse fra Databeskyttelsesrådet.

I forordningens artikel 46, stk. 3, er litra a en videreførelse af gældende ret for så vidt angår dataansvarlige. Nyt er det dog, at en ad hoc kontrakt efter litra a også kan indgås mellem en databehandler og en modtager i et tredjeland. Tilføjelsen af *databehandlere* må, som nævnt ovenfor, antages at hænge sammen med reglen i databeskyttelsesforordningens artikel 28, stk. 4. Reglen i litra b er ny.

Bestemmelsen i artikel 46, stk. 4, om anvendelse af sammenhængsmekanismen, er ny.

Endelig fastslås det i artikel 46, stk. 5, at godkendelser fra en medlemsstat eller tilsynsmyndighed på grundlag af artikel 26, stk. 2, i databeskyttelsesdirektivet i udgangspunktet også vil være gyldige, når forordningen finder anvendelse.

6.4. Bindende virksomhedsregler, artikel 47

6.4.1. Præsentation

Hverken databeskyttelsesdirektivet eller persondataloven indeholder i dag specifikke regler om bindende virksomhedsregler.

Artikel 29-gruppen har imidlertid flere gange udtalt sig om bindende virksomhedsregler. Gruppen har i sine udtalelser bl.a. forholdt sig til, i hvilket omfang bindende virksomhedsregler kan benyttes til at yde de tilstrækkelige garantier for beskyttelse af de registreredes rettigheder, der, efter databeskyttelsesdirektivets artikel 26, stk. 2 (persondatalovens § 27, stk. 4), kræves, hvis der ønskes overført personoplysninger til et tredjeland.

Når Artikel 29-gruppen i ovennævnte udtalelser har valgt – ret indgående – at udtale sig om bindende virksomhedsregler, skyldes dette bl.a., at gruppen har vurderet, at der er behov for, at internationale koncerner anlægger en global tilgang til databeskyttelse. Det er derfor nødvendigt at give koncernerne lov til at vedtage bindende interne regler, der regulerer overførsler af personoplysninger, som bliver behandlet af koncernen som *dataansvarlig*, mellem virksomheder inden for samme koncern.[706] Tilsvarende har internationale koncerner ad flere omgange bekræftet over for Artikel 29-gruppen, at bindende virksomhedsregler er et instrument, der matcher koncernernes ønsker i forhold til overførsel af person-

[706] Se bl.a. side 4 ff. i Artikel 29-gruppens udtalelse af 19. april 2013 om redegørelse vedrørende bindende virksomhedsregler for databehandlere (WP 204).

oplysninger til tredjelande. Som følge heraf har bindende virksomhedsregler i de senere år også vundet stadig større indpas blandt internationale koncerner.

I 2012 valgte Artikel 29-gruppen endvidere at åbne op for, at også koncerner – der alene virker som *databehandlere* – kan vedtage et sæt bindende virksomhedsregler med henblik på at yde sådanne tilstrækkelige garantier som nævnt i databeskyttelsesdirektivets artikel 26, stk. 2, når der på den dataansvarliges vegne overføres personoplysninger mellem virksomheder i databehandlerens koncern. Muligheden – der har kunnet anvendes siden 1. januar 2013 – var bl.a. begrundet i et konsekvent fremsat ønske fra især store koncerner i outsourcing-sektoren. Disse koncerner havde, i lighed med andre internationale koncerner, et stort ønske om at kunne anlægge en global tilgang til databeskyttelse, hvilket et instrument som bindende virksomhedsregler ville kunne muliggøre.

Som *bilag 1* er der vedlagt to figurer, der viser, hvordan kompleksiteten af en international koncerns overførsel af personoplysninger, til koncernvirksomheder i tredjelande, bliver mindre, når der benyttes bindende virksomhedsregler.

Med databeskyttelsesforordningens artikel 47 synes EU-lovgiver umiddelbart at støtte op om Artikel 29-gruppens hidtidige praksis vedrørende bindende virksomhedsregler, idet artikel 47 i vidt omfang – i hvert fald i forhold til de indholdsmæssige minimumskrav til et sæt bindende virksomhedsregler – er udtryk for en kodificering af Artikel 29-gruppens udtalelser.

6.4.2. Gældende ret

6.4.2.1. Begrebet "bindende virksomhedsregler"

Som nævnt ovenfor indeholder hverken databeskyttelsesdirektivet eller persondataloven specifikke regler om bindende virksomhedsregler. Gældende ret indeholder derfor heller ingen legal definition af, hvad et sæt bindende virksomhedsregler er.

På side 8 i en udtalelse af 3. juni 2003 om overførsel af personoplysninger til tredjelande i medfør af databeskyttelsesdirektivets artikel 26, stk. 2, ved brug af bindende virksomhedsregler (WP 74) har Artikel 29-gruppen dog givet gruppens bud på en treleddet definition af begrebet.

Artikel 29-gruppen definerer således bindende virksomhedsregler som 1) bindende regler i en international koncern, der 2) skal sikre tilstrækkelige garantier for beskyttelse af privatlivets fred, personers grundlæggende rettigheder og frihedsrettigheder samt for udøvelsen af de dertil knyttede rettigheder ved 3) overførsel til tredjelande.

6.4.2.2. Tilladelse til overførsel af personoplysninger til tredjelande baseret på godkendte bindende virksomhedsregler

6.4.2.2.1. Tilladelse efter persondatalovens § 27, stk. 4, til at overføre personoplysninger til tredjelande

6.4.2.2.1.1. Tilladelse når der er tale om bindende virksomhedsregler for dataansvarlige[707]

Af persondatalovens § 27, stk. 4, fremgår det bl.a., at Datatilsynet uden for de i stk. 3 nævnte tilfælde kan give tilladelse til, at der overføres oplysninger til tredjelande, som ikke opfylder stk. 1, såfremt den dataansvarlige yder tilstrækkelige garantier for beskyttelse af den registreredes rettigheder. Bestemmelsen bygger på artikel 26, stk. 2, i databeskyttelsesdirektivet.

For nærmere om persondatalovens § 27, stk. 4, henvises endvidere til afsnit 6.3. om overførsler omfattet af fornødne garantier, artikel 46.

En måde, hvorpå der i praksis kan ydes tilstrækkelige garantier for beskyttelse af den registreredes rettigheder efter persondatalovens § 27, stk. 4, er ved, at en dataansvarlig benytter sig af bindende virksomhedsregler.

Det er således muligt for en dansk virksomhed at få en tilladelse fra Datatilsynet til – i medfør af persondatalovens § 27, stk. 4 – at overføre virksomhedens egne personoplysninger til en virksomhed i et tredjeland, inden for samme koncern, baseret på bindende virksomhedsregler vedtaget af den dataansvarliges koncern.

I praksis forudsætter en tilladelse fra Datatilsynet til at overføre personoplysninger til tredjelande, baseret på bindende virksomhedsregler, at de bindende virksomhedsregler er blevet godkendt efter at have været underlagt en samarbejdsprocedure mellem de europæiske tilsynsmyndigheder.[708] Denne samarbejdsprocedure skal bl.a. sikre, at et sæt bindende virksomhedsregler lever op til en række indholdsmæssige minimumskrav. Samarbejdsproceduren og de indholdsmæssige minimumskrav til et sæt bindende virksomhedsregler vil blive gennemgået nedenfor.

Baggrunden for, at et sæt bindende virksomhedsregler skal godkendes efter en samarbejdsprocedure mellem de europæiske tilsynsmyndigheder, er, at bindende virksomhedsregler primært er tiltænkt anvendt af større internationale koncerner. Der vil derfor normalt ske overførsel af personoplysninger til tredjelande fra mange medlemsstater. Ved at benytte

[707] Bindende virksomhedsregler for dataansvarlige kaldes i daglig tale ofte for BCR-C (Binding Corporate Rules for Controllers).

[708] Med de europæiske tilsynsmyndigheder tænkes der her på tilsynsmyndighederne i de 28 EU-lande og i de 3 EØS lande, Norge Liechtenstein og Island.

samarbejdsproceduren sikres det, at der efterfølgende i alle medlemsstater[709] kan opnås tilladelse til at overføre personoplysninger til tredjelande baseret på de godkendte bindende virksomhedsregler.[710]

6.4.2.2.1.2. Tilladelse når der er tale om bindende virksomhedsregler for databehandlere[711]

I modsætning til bindende virksomhedsregler for dataansvarlige er bindende virksomhedsregler for databehandlere tænkt som et instrument, der kan anvendes i den situation, hvor personoplysninger behandles af en databehandler på vegne af en dansk dataansvarlig virksomhed og under dennes instruktioner, og hvor databehandleren ønsker at benytte underdatabehandlere inden for databehandlerens koncern. Som *bilag 2* er vedlagt en figur, der viser grundopbygningen af et sæt bindende virksomhedsregler for databehandlere.

Ved at udarbejde bindende virksomhedsregler for databehandlere vil databehandleren for det første kunne undgå, at der skal indgås databehandleraftaler mellem de dataansvarlige og hver enkelt virksomhed inden for databehandlerens koncern, hvilket for nogle virksomheder kan være rigtig mange kontrakter. Ligeledes vil databehandleren for det andet kunne undgå, at der skal tilvejebringes et særskilt overførselsgrundlag ved overførsel fra de dataansvarlige til hver enkelt koncernvirksomhed, herunder f.eks. ved brug af Kommissionens standardkontraktbestemmelser.

Instrumentet for bindende virksomhedsregler for databehandlere er opbygget således, at databehandlerkoncernens bindende virksomhedsregler skal vedlægges som et anneks til den databehandleraftale, der skal indgås mellem den dataansvarlige og databehandleren, jf. databeskyttelsesdirektivets artikel 17, stk. 3, som er gennemført i dansk ret ved persondatalovens § 42, stk. 2.

Databehandlerkoncernens bindende virksomhedsregler vil herefter kunne benyttes af en dansk dataansvarlig til i medfør af persondatalovens § 27, stk. 4, at ansøge om tilladelse fra Datatilsynet til at overføre virksomhedens egne personoplysninger til underdatabehandlere, inden for databehandlerens koncern, i tredjelande.

I praksis vil det ofte være databehandleren, der på vegne af den dataansvarlige ansøger Datatilsynet om tilladelse til at overføre personoplysninger til tredjelande. Dette skyldes, at bindende virksomhedsregler for databehandlere i vidt omfang bliver anvendt af store inter-

[709] Portugal er pt. den eneste EU-medlemsstat, hvori der ikke kan opnås tilladelse til at overføre personoplysninger til tredjelande baseret på et godkendt sæt bindende virksomhedsregler.
[710] Bemærk, at der ikke nødvendigvis er krav om specifik efterfølgende tilladelse i alle medlemsstater.
[711] Bindende virksomhedsregler for databehandlere kaldes i daglig tale ofte for BCR-P (Binding Corporate Rules for Processors).

nationale koncerner, der foretager databehandling for et stort antal dataansvarlige, herunder små virksomheder, der ikke umiddelbart selv har de juridiske kompetencer mv. til at ansøge om tilladelse.

Det er dog meget vigtigt at være opmærksom på, at det som udgangspunkt er de enkelte dataansvarlige (uanset om de måtte være i stand til fuldt ud at overskue et sæt bindende virksomhedsregler), der bevarer ansvaret for at sikre, at der ydes tilstrækkelige garantier for beskyttelse af de registreredes rettigheder ved overførsler inden for databehandlerkoncernen. Det er derfor som udgangspunkt også den dataansvarlige, der kan blive holdt ansvarlig for eventuelle brud på de vedtagne bindende virksomhedsregler samt databeskyttelseslovgivningen i øvrigt.

6.4.2.2.2. Samarbejde om godkendelse af bindende virksomhedsregler

Den samarbejdsprocedure mellem de europæiske tilsynsmyndigheder om godkendelse af bindende virksomhedsregler, der kort er omtalt ovenfor, er primært reguleret i en udtalelse fra Artikel 29-gruppen af 14. april 2005 om en samarbejdsprocedure vedrørende bindende virksomhedsregler (WP 107) og i en aftale om gensidig anerkendelse ("mutual recognition") mellem 21 tilsynsmyndigheder.

Samarbejdsproceduren anvendes uanset, om der ønskes godkendelse af bindende virksomhedsregler for dataansvarlige eller bindende virksomhedsregler for databehandlere. I praksis er det i øvrigt ikke sjældent, at en international koncern ønsker at få godkendt begge typer bindende virksomhedsregler.

I det følgende vil der kort blive redegjort for ovennævnte udtalelse fra Artikel 29-gruppen og aftalen om gensidig anerkendelse.

6.4.2.2.2.1. Artikel 29-gruppens udtalelse af 14. april 2005 (WP 107)

Af Artikel 29-gruppens udtalelse fremgår det bl.a., at den koncern, der ønsker at få godkendt et sæt bindende virksomhedsregler, på baggrund af nogle nærmere angivne kriterier, skal foreslå en tilsynsmyndighed i en enkelt medlemsstat – typisk tilsynsmyndigheden i det land hvor det europæiske hovedkvarter befinder sig – til at lede godkendelsesproceduren.

Den foreslåede ledende tilsynsmyndighed vil herefter kontakte de øvrige relevante tilsynsmyndigheder (tilsynsmyndighederne i de medlemsstater hvorfra der påtænkes overført oplysninger til tredjelande) og bede dem om – inden for en måned – at komme med indvendinger, hvis de ikke finder, at den foreslåede ledende tilsynsmyndighed er den rette.

Hvis der ikke kommer nogen indvendinger (hvilket der normalt ikke gør), vil den ledende tilsynsmyndighed herefter gennemgå de modtagne bindende virksomhedsregler og drøfte indholdet med ansøgerkoncernen.

Når den ledende tilsynsmyndighed er tilfreds med indholdet (finder, at de bindende virksomhedsregler lever op til de indholdsmæssige minimumskrav), sender den ledende tilsynsmyndighed de bindende virksomhedsregler i høring hos de øvrige relevante tilsynsmyndigheder.

Hvis den ledende tilsynsmyndighed modtager ønsker, fra de øvrige relevante tilsynsmyndigheder, om rettelser, præciseringer mv., vil den ledende tilsynsmyndighed videreformidle disse til ansøgerkoncernen og bede den om at forholde sig til ønskerne. Ansøgerkoncernens svar på de modtagne ønsker sendes herefter retur til de relevante tilsynsmyndigheder til eventuel kommentering.

Når alle relevante tilsynsmyndigheder er tilfredse med de bindende virksomhedsreglers indhold, vil den ledende tilsynsmyndighed sende den endelige version til de andre tilsyn. Denne endelige version kan derefter danne grundlag for nationale udtalelser og tilladelser, hvor dette er påkrævet. Artikel 29-gruppen og Kommissionen bliver underrettet, når WP 107 proceduren er tilendebragt.

6.4.2.2.2.2. Aftalen om gensidig anerkendelse mellem 21 tilsynsmyndigheder

Som følge af et ønske, fra både internationale koncerner og flere tilsynsmyndigheder, om en hurtigere og mere effektiv behandling af ansøgninger om godkendelse af bindende virksomhedsregler valgte en række tilsynsmyndigheder i 2008 at indgå en aftale om gensidig anerkendelse.

Aftalen indebærer, at de deltagende tilsynsmyndigheder forpligter sig til at lægge den ledende tilsynsmyndigheds vurdering til grund. De deltagende tilsynsmyndigheder vil således ikke – som Artikel 29-gruppens udtalelse i WP 107 ellers tilsiger det – modtage de bindende virksomhedsregler til kommentering, men vil blot modtage den endelige version fra den ledende tilsynsmyndighed og derefter give de fornødne nationale tilladelser baseret på dennes vurdering.

I praksis vil den ledende tilsynsmyndighed normalt bede to såkaldte ”co-reviewers” om at gennemgå de bindende virksomhedsregler, når den finder, at de lever op til de indholdsmæssige minimumskrav. Dette sker som en slags ekstra kontrol, og initiativet fik i øvrigt flere tilsynsmyndigheder til at tilslutte sig aftalen om gensidig anerkendelse.

Som nævnt ovenfor har pt. 21 lande tilsluttet sig aftalen om gensidig anerkendelse. Se mere herom i *bilag 3* til dette afsnit.

Datatilsynet har ikke tilsluttet sig aftalen om gensidig anerkendelse, idet dette efter tilsynets opfattelse ikke vil være foreneligt med persondatalovens § 27, stk. 4, samt det forvaltningsretlige officialprincip. Dog har Datatilsynet meddelt de øvrige tilsynsmyndigheder, at de oplysninger og tilkendegivelser, som Datatilsynet modtager fra den ledende tilsynsmyndighed vil blive tillagt betydelig vægt i tilsynets vurdering af et sæt bindende virksomhedsregler.

Det, at 21 tilsynsmyndigheder deltager i aftalen om gensidig anerkendelse, betyder i praksis, at der er markant færre tilsynsmyndigheder, der skal involveres i samarbejdsproceduren for godkendelse af bindende virksomhedsregler. Hvis den franske tilsynsmyndighed (som har tilsluttet sig aftalen om gensidig anerkendelse) f.eks. fungerer som ledende tilsynsmyndighed, kan denne nøjes med at forelægge de bindende virksomhedsregler for helt ned til ni ud af 30 mulige tilsynsmyndigheder.[712] En forudsætning for at komme helt ned på ni tilsynsmyndigheder er dog, at den franske tilsynsmyndighed vælger to af de tilsynsmyndigheder, der ikke har tilsluttet sig aftalen om gensidig anerkendelse, som co-reviewers.

6.4.2.2.3. Kort om udviklingen i antallet af sager i Datatilsynet siden Artikel 29-gruppen med WP 107 åbnede op for brugen af bindende virksomhedsregler

Datatilsynet gav den 24. marts 2006 sin første tilladelse til, at en dansk virksomhed kunne overføre personoplysninger til tredjelande ved at yde sådanne tilstrækkelige garantier som nævnt i persondatalovens § 27, stk. 4, i form af bindende virksomhedsregler.

Efterfølgende har Datatilsynet behandlet en lang række sager vedrørende overførsel af personoplysninger til tredjelande i medfør af persondatalovens § 27, stk. 4, baseret på virksomheders bindende virksomhedsregler – fra 1. januar 2013 også bindende virksomhedsregler for databehandlere.[713]

Siden 2009 har Datatilsynet endvidere været (eller er) ledende tilsynsmyndighed i otte sager, hvoraf de fem[714] indtil videre er afsluttet og er resulteret i tilladelser til, at danske virksomheder kan overføre personoplysninger til tredjelande baseret på en dansk international koncerns bindende virksomhedsregler.

[712] Alle EU-medlemsstater med undtagelse af Portugal og de tre EØS-lande.
[713] Datatilsynet har pt. behandlet mere end 80 sager.
[714] Datatilsynets j.nr. 2009-841-0057 (Novo Nordisk A/S), 2012-841-0011 (A.P. Møller-Mærsk A/S), 2012-841-0025 (Rockwool A/S), 2013-847-0074 (Lego System A/S) og 2015-847-0074 (Danfoss A/S).

6.4.2.3. De indholdsmæssige minimumskrav til et sæt bindende virksomhedsregler

Som nævnt ovenfor i afsnit har Artikel 29-gruppen i en række udtalelser forholdt sig til muligheden for at overføre personoplysninger til tredjelande i medfør af databeskyttelsesdirektivets artikel 26, stk. 2 (persondatalovens § 27, stk. 4), ved at benytte bindende virksomhedsregler til at yde tilstrækkelige garantier for beskyttelse af de registreredes rettigheder.

Langt de fleste af Artikel 29-gruppens udtalelser angår de indholdsmæssige minimumskrav til bindende virksomhedsregler, og der er i vidt omfang overlap mellem flere af udtalelserne.

I den følgende beskrivelse af de indholdsmæssige minimumskrav til bindende virksomhedsregler vil der blive taget udgangspunkt i Artikel 29-gruppens udtalelser i WP 133[715] og WP 153[716] for så vidt angår bindende virksomhedsregler for dataansvarlige og WP 195[717] og WP 195a[718] for så vidt angår bindende virksomhedsregler for databehandlere. De resterende af Artikel 29-gruppens udtalelser vil ikke blive nærmere omtalt.[719]

6.4.2.3.1. Bindende virksomhedsregler for dataansvarlige

Ved en gennemgang af Artikel 29-gruppens udtalelser kan det konstateres, at gruppen opstiller en række indholdsmæssige minimumskrav i forhold til, hvad der skal fremgå af henholdsvis virksomhedens ansøgningsblanket og af virksomhedens bindende virksomhedsregler.

Minimumskravene til indholdet af ansøgningsblanketten og et sæt bindende virksomhedsregler for dataansvarlige bliver nærmere beskrevet i skemaet i *bilag 4.*

Grundlæggende kan kravene til et sæt bindende virksomhedsregler inddeles i følgende seks kategorier: 1) Krav om bindende virkning, 2) krav om efterlevelse, 3) krav om samarbejdsforpligtelse, 4) krav om beskrivelse af behandlinger og data flows, 5) krav om mekanisme til rapportering af ændringer og 6) krav til databeskyttelse.

---

[715] Artikel 29-gruppens udtalelse af 10. januar 2007 om standardansøgningsblanket ved godkendelse af bindende virksomhedsregler for dataansvarlige (WP 133).

[716] Artikel 29-gruppens udtalelse af 24. juni 2008 om elementer og principper, der skal være indeholdt i et sæt bindende virksomhedsregler for dataansvarlige (WP 153).

[717] Artikel 29-gruppens udtalelse af 6. juni 2012 om elementer og principper, der skal være indeholdt i et sæt bindende virksomhedsregler for databehandlere (WP 195).

[718] Artikel 29-gruppens udtalelse af 17. september 2012 om standardansøgningsblanket ved godkendelse af bindende virksomhedsregler for databehandlere (WP 195a).

[719] WP 74 om introduktion af bindende virksomhedsregler og indhold, WP 108 om tjekliste ved ansøgning, WP 154 om eksempel på struktur, WP 155 om FAQ og WP 204 om redegørelse vedrørende bindende virksomhedsregler for databehandlere.

6.4.2.3.2. Bindende virksomhedsregler for databehandlere
Som det det er tilfældet med bindende virksomhedsregler for dataansvarlige, opstiller Artikel 29-gruppen også, i forhold til bindende virksomhedsregler for databehandlere, en række indholdsmæssige minimumskrav med hensyn til, hvad der skal fremgå af henholdsvis virksomhedens ansøgningsblanket og af virksomhedens bindende virksomhedsregler.

Minimumskravene til bindende virksomhedsregler for databehandlere minder om kravene til bindende virksomhedsregler for dataansvarlige, og strukturen er også den samme. Der er imidlertid foretaget en del indholdsmæssige ændringer, som har været nødvendiggjort af, at bindende virksomhedsregler for databehandlere på en række punkter grundlæggende adskiller sig fra bindende virksomhedsregler for dataansvarlige. Minimumskravene kan dog også her inddeles i de ovenfor beskrevne seks kategorier.

Minimumskravene til indholdet af ansøgningsblanketten og et sæt bindende virksomhedsregler for databehandlere er nærmere beskrevet i skemaet i *bilag 5.*

6.4.3. Databeskyttelsesforordningen
6.4.3.1. Begrebet bindende virksomhedsregler
I databeskyttelsesforordningens artikel 4, nr. 20, defineres bindende virksomhedsregler 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.

Selvom Artikel 29-gruppens definition af bindende virksomhedsregler fra 2003, i sin ordlyd, ikke er identisk med ordlyden i databeskyttelsesforordningens artikel 4, nr. 20, er der næppe med forordningen tiltænkt en ændret forståelse af begrebet.

6.4.3.2. Databeskyttelsesforordningens artikel 47, stk. 1
Det fremgår af databeskyttelsesforordningens artikel 47, stk. 1, at den kompetente tilsynsmyndighed, i overensstemmelse med den sammenhængsmekanisme, der er omhandlet i artikel 63, godkender bindende virksomhedsregler, såfremt de:

> a) er retligt bindende og gælder for og håndhæves af alle berørte medlemmer i den koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet, herunder deres medarbejdere

b) udtrykkeligt tillægger registrerede rettigheder, som kan håndhæves, for så vidt angår behandling af deres personoplysninger, og

c) opfylder kravene i stk. 2.

Endvidere fremgår det af 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.

Forordningens artikel 47, stk. 1, indebærer som noget nyt, at det fremadrettet kun er den kompetente tilsynsmyndighed (typisk tilsynsmyndigheden i den medlemsstat, hvori koncernens EU hovedkvarter er beliggende), der skal godkende et sæt bindende virksomhedsregler.

De øvrige berørte tilsynsmyndigheder skal således ikke længere (hvor dette måtte have været et nationalt krav tidligere) give specifik tilladelse til, at koncernvirksomheder, beliggende i den pågældende tilsynsmyndigheds medlemsstat, må overføre personoplysninger til tredjelande baseret på bindende virksomhedsregler. Dette fremgår også af databeskyttelsesforordningens artikel 46, stk. 2, litra b.

At det fremover kun er den kompetente tilsynsmyndighed, der skal godkende et sæt bindende virksomhedsregler, må forventes at indebære, at godkendelsesprocessen bliver mere smidig, idet en ansøgerkoncern ikke længere skal forholde sig til forskellige fortolkninger og implementeringer hos tilsynene i de enkelte medlemsstater.

Endvidere er det nyt, at den kompetente tilsynsmyndighed *skal* godkende et sæt bindende virksomhedsregler, hvis de krav, der bliver oplistet i bestemmelsen, er opfyldt. Tidligere var der nok mere plads til fortolkning, da tilsynsmyndighedernes vurdering alene gik på, om der blev ydet tilstrækkelige garantier for beskyttelse af de registreredes rettigheder, jf. databeskyttelsesdirektivets artikel 26, stk. 2.

Det, at muligheden for fortolkning bliver indsnævret, vil formentlig også gøre godkendelsesprocessen mere smidig for ansøgerkoncernerne. Med forordningen ved ansøger således, at der kan forventes en godkendelse, hvis de bindende virksomhedsregler lever op til en række oplistede minimumskrav.

I forhold til samarbejdet mellem tilsynsmyndighederne om godkendelse af bindende virksomhedsregler, bliver det omtalte samarbejde erstattet af, at bindende virksomhedsregler fremover skal behandles efter sammenhængsmekanismen i forordningens artikel 63. Dette betyder bl.a., at den kompetente tilsynsmyndighed skal have en forudgående udtalelse fra Databeskyttelsesrådet – efter artikel 64, stk. 1, litra f – inden den godkender et sæt bindende virksomhedsregler.

Det må umiddelbart antages at ville kunne føre til kortere sagsbehandlingstider, at tilsynsmyndighederne fremadrettet skal samarbejde efter reglerne i forordningens kapitel VII, afdeling 2, i stedet for den omtalte procedure. Dette skyldes bl.a., at der i forordningens artikel 64, stk. 3, fastsættes relativt korte frister for, hvornår Databeskyttelsesrådets udtalelse senest skal foreligge, ligesom rådet kan vedtage deres udtalelse med simpelt flertal. Uenigheder mellem tilsynsmyndighederne vil derfor, med den nye ordning, ikke i samme omfang som hidtil skulle landes på et kompromis, hvilket i praksis kunne tage tid.

6.4.3.3. Databeskyttelsesforordningens artikel 47, stk. 2

Af databeskyttelsesforordningens artikel 47, stk. 2, fremgår det, at de bindende virksomhedsregler i stk. 1 mindst skal angive:

> a) strukturen i og kontaktoplysningerne for den koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet, og hvert af dens medlemmer
>
> b) overførslerne eller rækken af overførsler af oplysninger, herunder kategorier af personoplysninger, behandlingstype og -formål, typen af berørte registrerede og angivelse af det pågældende tredjeland eller de pågældende tredjelande
>
> c) deres retligt bindende karakter, både internt og eksternt
>
> d) anvendelsen af de generelle databeskyttelsesprincipper, navnlig formålsbegrænsning, dataminimering, begrænsede opbevaringsperioder, datakvalitet, databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, retsgrundlag for behandling, behandling af særlige kategorier af personoplysninger, foranstaltninger til at sikre datasikkerhed og krav til videreoverførsel til organer, der ikke er underlagt de bindende virksomhedsregler

e) de registreredes rettigheder med hensyn til behandling og midler til at udøve disse rettigheder, herunder til ikke at blive gjort til genstand for afgørelser, som alene er truffet på grundlag af automatisk behandling, herunder profilering, jf. artikel 22, samt retten til at indgive klage til den kompetente tilsynsmyndighed og de kompetente domstole i medlemsstaterne, jf. artikel 79, og til at modtage godtgørelse og, hvis det er relevant, erstatning for brud på de bindende virksomhedsregler

f) den dataansvarliges eller databehandlerens accept af ansvaret for ethvert brud på de bindende virksomhedsregler, der begås af en berørt virksomhed i koncernen, som ikke er etableret i Unionen, når den dataansvarlige eller databehandleren er etableret inden for en medlemsstats område; den dataansvarlige eller databehandleren fritages kun helt eller delvis for dette ansvar, hvis vedkommende beviser, at den pågældende virksomhed ikke er skyld i den begivenhed, der medførte skaden

g) hvordan informationen om bindende virksomhedsregler, navnlig de bestemmelser, der er omhandlet i litra d), e) og f), gives til de registrerede ud over den information, der er omhandlet i artikel 13 og 14

h) opgaverne for enhver databeskyttelsesrådgiver, der er udpeget i henhold til artikel 37, eller enhver anden person eller enhed med ansvar for overvågning af overholdelse af de bindende virksomhedsregler inden for koncernen eller gruppen af foretagender, der udøver en fælles økonomisk aktivitet, samt overvågning af uddannelse og håndtering af klager

i) klageprocedurerne

j) de mekanismer i koncernen eller gruppen af foretagender, der udøver en fælles økonomisk aktivitet, som skal sikre kontrol af overholdelse af de bindende virksomhedsregler. Sådanne mekanismer skal omfatte databeskyttelsesrevisioner og metoder til at sikre korrigerende foranstaltninger med henblik på at beskytte de registreredes rettigheder. Resultaterne af denne revision bør meddeles den person eller enhed, der er omhandlet i litra h), og bestyrelsen i kontrolvirksomheden i en koncern eller i gruppen af foretagender, der udøver en fælles økonomisk aktivitet, og bør være tilgængelige på anmodning af den kompetente tilsynsmyndighed

k) mekanismerne til indberetning og registrering af ændringer af reglerne og indberetning af disse ændringer til tilsynsmyndigheden

l) den mekanisme til samarbejde med tilsynsmyndigheden, som har til formål at sikre, at alle virksomheder i koncernen eller gruppen af foretagender, der udøver en fælles økonomisk aktivitet, overholder reglerne, navnlig ved at forelægge tilsynsmyndigheden resultaterne af revisionen af de foranstaltninger, der er omhandlet i litra j)

m) mekanismerne til indberetning til den kompetente tilsynsmyndighed af retlige forpligtelser, som en virksomhed i koncernen eller gruppen af foretagender, der udøver en fælles økonomisk aktivitet, er omfattet af i et tredjeland, og som sandsynligvis vil have betydelig negativ indvirkning på garantierne i de bindende virksomhedsregler, og

n) den passende databeskyttelsesuddannelse, som personale, der har permanent eller regelmæssig adgang til personoplysninger, skal følge.

Når minimumskravene i databeskyttelsesforordningens artikel 47, stk. 2, sammenholdes med de eksisterende minimumskrav i Artikel 29-gruppens udtalelser, kan det konstateres, at kravene i artikel 47, stk. 2, litra a-c, e-g og i-n, stort set er identiske med de minimumskrav, der følger af Artikel 29-gruppens udtalelser, om end Artikel 29-gruppen beskriver visse af kravene mere udførligt.

Forordningens artikel 47, stk. 2, litra d, er en delvis videreførelse af gældende ret, men henvisningen til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er udtryk for en nyskabelse og en konsekvens af de eksplicitte krav herom i forordningens artikel 25.

Artikel 47, stk. 2, litra h, er ny i den forstand, at opgaverne for enhver databeskyttelsesrådgiver bindes op på en specifik bestemmelse i forordningens artikel 37 om udpegelse af databeskyttelsesrådgiver. Det er dog ikke nyt, at en koncern skal udpege en databeskyttelsesrådgiver, som skal efterse, om de bindende virksomhedsregler bliver iagttaget i koncernen.

6.4.3.4. Databeskyttelsesforordningens artikel 47, stk. 3

Det fremgår af databeskyttelsesforordningens artikel 47, stk. 3, at Kommissionen kan angive formatet og procedurerne for udveksling af oplysninger mellem dataansvarlige, data-

behandlere og tilsynsmyndigheder for bindende virksomhedsregler som omhandlet i denne artikel.

Endvidere fremgår det, at disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

Det må forventes, at Kommissionen vil benytte sin kompetence efter artikel 47, stk. 3, til at præcisere, hvad der nærmere ligger i kravene i artikel 47, stk. 2. I den forbindelse må det ligeledes forventes, at Kommissionen i vidt omfang vil skele til Artikel 29-gruppens udtalelser om bindende virksomhedsregler.

6.4.3.5. Databeskyttelsesforordningens artikel 70, stk. 1, litra i

Af databeskyttelsesforordningens artikel 70, stk. 1, litra i, fremgår det, at Databeskyttelsesrådet skal udstede retningslinjer, henstillinger og bedste praksis i overensstemmelse med dette stykkes litra e) med henblik på nærmere at angive kriterierne for og kravene til overførsel af personoplysninger baseret på bindende virksomhedsregler, som dataansvarlige overholder, og bindende virksomhedsregler, som databehandlere overholder, og vedrørende yderligere krav til at sikre beskyttelse af de berørte registreredes personoplysninger som omhandlet i artikel 47.

Med denne bestemmelse videreføres gældende ret, hvorefter Artikel 29-gruppen løbende har udtalt sig om krav mv. i forhold til overførsel af personoplysninger til tredjelande baseret på bindende virksomhedsregler. Databeskyttelsesrådets kommende retningslinjer og henstillinger vil dog skulle kunne rummes inden for bestemmelserne i artikel 47.

6.4.4. Overvejelser

Med databeskyttelsesforordningens artikel 47 fastsættes der, som noget nyt, udtrykkelige regler om bindende virksomhedsregler.

Reglerne i artikel 47 er dog i vidt omfang – i hvert fald i forhold til de indholdsmæssige minimumskrav til et sæt bindende virksomhedsregler – udtryk for en kodificering af en række udtalelser fra Artikel 29-gruppen om brugen af bindende virksomhedsregler, som overførselsgrundlag, i forbindelse med EU koncernvirksomheders overførsel af personoplysninger til andre koncernvirksomheder beliggende i tredjelande.

For så vidt angår proceduren for godkendelse af et sæt bindende virksomhedsregler, er det nyt, at det fremadrettet kun er den kompetente tilsynsmyndighed (typisk tilsynsmyndigheden i den medlemsstat, hvori koncernens EU hovedkvarter er beliggende), der skal godkende et sæt bindende virksomhedsregler.

Det er endvidere nyt, at den kompetente tilsynsmyndighed *skal* godkende et sæt bindende virksomhedsregler, hvis de krav, der bliver oplistet i bestemmelsen, er opfyldt.

Endelig er det nyt, at den eksisterende procedure for samarbejde, mellem tilsynsmyndighederne, om godkendelse af bindende virksomhedsregler, vil blive erstattet af reglerne i databeskyttelsesforordningens kapitel VII, afdeling 2, om sammenhængsmekanisme mv.

Det må forventes, at ovennævnte nye procedurer for godkendelse og samarbejde vil føre til, at processen for godkendelse af et sæt bindende virksomhedsregler bliver mere smidig, hvilket vil være en fordel for koncerner, der i fremtiden ønsker at ansøge om godkendelse af et sæt bindende virksomhedsregler.

For så vidt angår de indholdsmæssige minimumskrav til et sæt bindende virksomhedsregler, er reglerne i forordningens artikel 47, stk. 2, næsten identiske med de minimumskrav, der følger af Artikel 29-gruppens udtalelser, om end Artikel 29-gruppen beskriver visse af kravene mere udførligt.

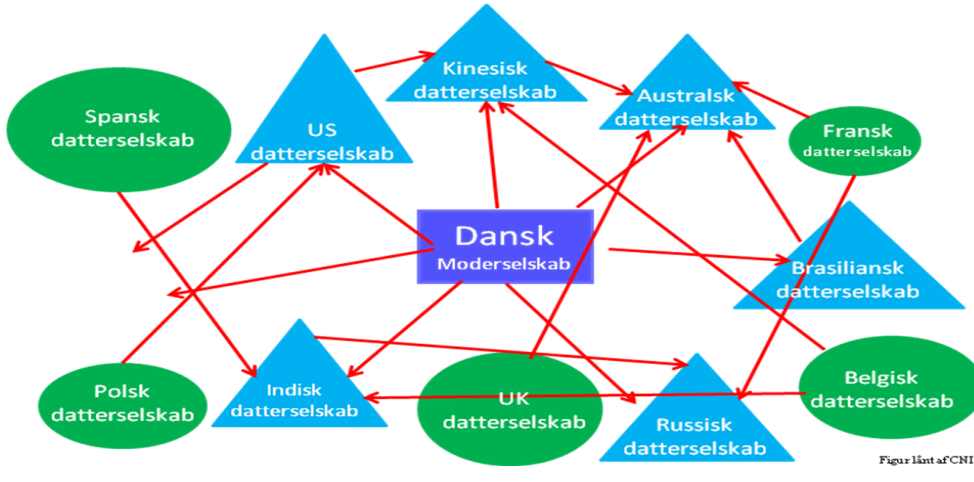
Bestemmelsen i forordningens artikel 47, stk. 2, litra d, er dog kun en delvis videreførelse af gældende ret, idet der, som noget nyt, eksplicit indsættes databeskyttelsesprincipper i form af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

I forordningens artikel 47, stk. 2, litra h, er det endvidere nyt, at opgaverne for enhver databeskyttelsesrådgiver bindes op på en specifik bestemmelse i forordningens artikel 36 om udpegelse af databeskyttelsesrådgiver. Selve det materielle indhold er dog ikke nyt.

Bilag 1 – to figurer der viser, hvordan kompleksiteten af en international koncerns overførsel af personoplysninger, til koncernvirksomheder i tredjelande, bliver mindre, når der benyttes bindende virksomhedsregler.

A) Koncern der ikke benytter bindende virksomhedsregler

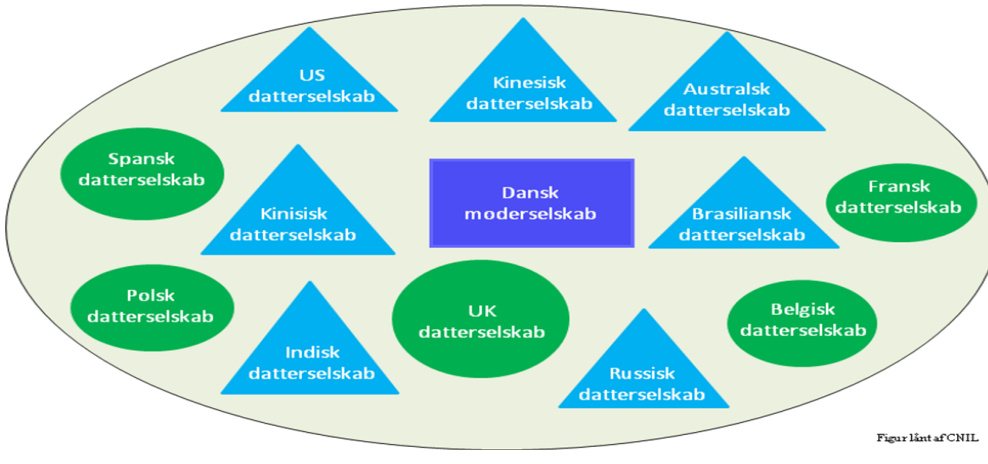
Nedenstående figur er et eksempel på kompleksiteten i forhold til overførsel af personoplysninger i en koncern, der ikke benytter bindende virksomhedsregler. Når der ikke benyttes bindende virksomhedsregler, vil der skulle tilvejebringes et særskilt overførselsgrundlag hver gang en koncernvirksomhed i EU ønsker at overføre oplysninger til en koncernvirksomhed uden for EU. Disse overførselsgrundlag kan bl.a. være Kommissionens standardkontraktbestemmelser, ad hoc kontrakter eller undtagelserne i persondatalovens § 27, stk. 3.



Figur lånt af CNIL

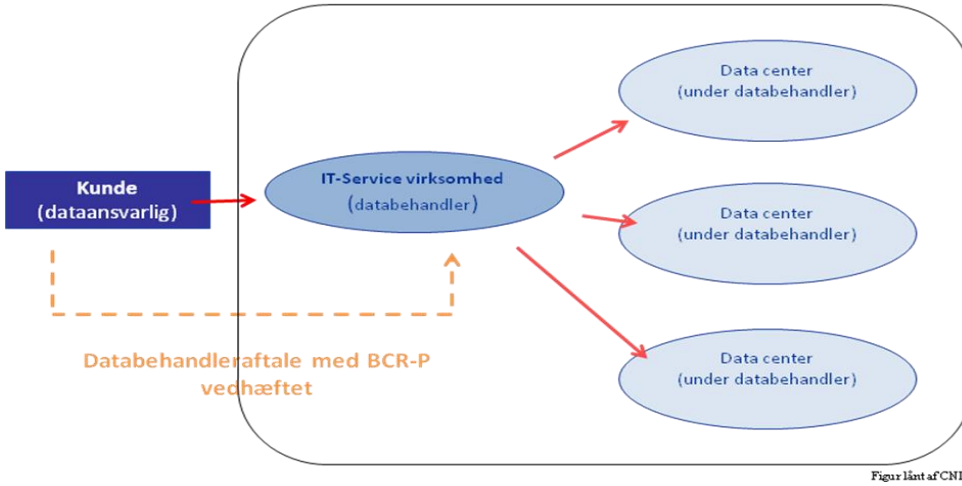
B) Koncern der benytter bindende virksomhedsregler

Nedenstående figur viser, hvordan kompleksiteten i forhold til overførsel af personoplysninger til tredjelande bliver mindre, hvis koncernen beskrevet ovenfor under punkt A benytter sig af bindende virksomhedsregler. Med vedtagelsen af bindende virksomhedsregler bliver niveauet af databeskyttelse i de koncernvirksomheder, der er beliggende i tredjelande, løftet op, så overførsel af personoplysninger til disse fra koncernvirksomheder i EU ikke længere kræver et særskilt overførselsgrundlag.



Figur lånt af CNIL

Bilag 2 – figur der viser grundopbygningen af et sæt bindende virksomhedsregler for databehandlere



Figur lånt af CNIL

Bilag 3 – figur der viser hvilke lande, der har tilsluttet sig aftalen om gensidig anerkendelse

MR procedure

Belgien, Bulgarien, Cypern, Estland, Frankrig, Holland, Irland, Italien, Letland, Luxembourg, Malta, Slovakiet, Slovenien, Spanien, Tjekkiet, Tyskland, UK og Østrig.

+ Island, Liechtenstein og Norge

Co-operation procedure

Danmark, Finland, Grækenland, Kroatien, Litaun, Polen, Rumænien, Sverige og Ungarn

Bemærk: BCR er ikke anvendelig I Portugal

Figur lånt af CNIL

Bilag 4 – skema over indholdsmæssige minimumskrav til et sæt bindende virksomhedsregler for dataansvarlige

Skemaet er baseret på Artikel 29-gruppens udtalelse i WP 153. Bemærk venligst, at nedenstående ikke er en 1:1 oversættelse af den officielle engelske version. En koncern, der ønsker at udarbejde et sæt bindende virksomhedsregler, bør derfor også læse den officielle tekst.

Indholdsmæssige minimumskrav	I de bindende virksomhedsregler	I ansøgningsblanketten	Bemærkninger
1. Bindende virkning			
Internt i koncernen			
1.1. Forpligtelse til at respektere de bindende virksomhedsregler	Ja	Ja	De bindende virksomhedsregler skal indeholde en klar forpligtelse for alle koncernvirksomheder og for alle ansatte til at respektere de bindende virksomhedsregler
1.2. En redegørelse for hvordan reglerne er gjort bindende for koncernvirksomhederne og de ansatte	Nej	Ja	I forhold til koncernvirksomhederne kan reglerne f.eks. være blevet gjort bindende ved aftaler mellem koncernvirksomhederne eller ved hjælp af ensidige erklæringer fra "modervirksomheden". I forhold til de ansatte kan reglerne f.eks. være blevet gjort bindende via tillæg til ansættelseskontrakter eller via interne politikker udstykket af ledelsen. Manglende iagttagelse skal være sanktioneret.
Eksternt			
1.3. Fastsættelse af tredjepartsrettigheder	Ja	Ja	De bindende virksomhedsregler skal give de registrerede mulig-

for de registrerede, herunder retten til at klage til en relevant tilsynsmyndighed eller indbringe en klage for domstolene (kan vælge mellem jurisdiktionen for EU dataeksportøren eller jurisdiktionen for koncernens EU hovedkvarter).			hed for at håndhæve reglerne som begunstigede tredjeparter. Tredjepartsrettighederne bør inkludere retten til klageadgang og retten til at modtage erstatning (jf. artikel 22 og 23 i databeskyttelsesdirektivet).
1.4. Koncernen accepterer at hæfte for at betale erstatning og for at afhjælpe brud på reglerne.	Ja	Ja	De bindende virksomhedsregler skal indeholde en forpligtelse for koncernens EU hovedkvarter, eller den EU koncernvirksomhed, der har accepteret ansvaret, for at hæfte for brud på de bindende virksomhedsregler begået af koncernvirksomheder i tredjelande. Det skal endvidere fremgå af de bindende virksomhedsregler, at domstolene eller andre kompetente myndigheder i EU har jurisdiktion, hvis en koncernvirksomhed uden for EU handler i strid med reglerne. Hvis det i en koncern ikke måtte være muligt for en enkelt koncernvirksomhed at påtage sig ansvaret for alle brud på reglerne uden for EU, kan tilsynsmyndighederne acceptere andre hæftelsesmekanismer, hvis der stilles fornødne garantier for, at de registrerede fortsat kan håndhæ-

			ve deres rettigheder på en betryggende måde. En mulighed kan f.eks. være delt ansvar mellem EU dataeksportøren og dataimportøren i et tredjeland.
1.5. Koncernen har de fornødne aktiver	Nej	Ja	I ansøgningsblanketten skal det bekræftes, at den EU koncernvirksomhed, der har accepteret at hæfte for brud på reglerne uden for EU, har de fornødne aktiver til at betale eventuel erstatning mv.
1.6. Koncernen har bevisbyrden	Ja	Ja	Det skal fremgå af de bindende virksomhedsregler, at den EU koncernvirksomhed, der har accepteret at hæfte for brud på reglerne uden for EU, har bevisbyrden for, at en koncernvirksomhed uden for EU ikke er ansvarlig for et brud på reglerne, som har resulteret i, at en registreret søger erstatning. Kan det dokumenteres, at en koncernvirksomhed uden for EU ikke er ansvarlig for et brud, kan den EU koncernvirksomhed, der har accepteret at hæfte for eventuelle brud, også frasige sig ansvaret.
1.7. De registrerede har let adgang til de bindende virksomhedsregler, herunder i sær information om de registreredes tredjepartsrettigheder, og hvordan de kan påberåbe sig dem.	Ja	Nej	De bindende virksomhedsregler skal give de registrerede mulighed for at let at tilgå indholdet af disse. For eksempel kan det fremgå af de bindende virksomhedsregler, at disse vil blive gjort tilgænge-

			lige på internettet eller på et intranet (hvis de registrerede er ansatte).
2. Efterlevelse			
2.1. Der skal være et passende uddannelsesprogram	Ja	Ja	Det skal fremgå af de bindende virksomhedsregler, at ansatte, der permanent eller regelmæssigt behandler personoplysninger, vil skulle gennemgå et passende uddannelsesprogram i forhold til de bindende virksomhedsregler. Typisk vil det være en fordel at vedlægge eksempler på, hvordan de ansatte vil modtage den fornødne uddannelse.
2.2. Der skal være en klagebehandlingsprocedure	Ja	Ja	Et sæt bindende virksomhedsregler skal indeholde en intern klagebehandlingsprocedure, som de registrerede kan benytte, hvis de finder, at en koncernvirksomhed ikke efterlever reglerne. Klager skal håndteres af en nem identificerbar afdeling eller person, som har den fornødne uafhængighed fra resten af koncernen. I ansøgningsblanketten skal det beskrives, hvordan de registrerede vil blive informeret om klagebehandlingsproceduren, herunder om, hvortil der kan klages, i hvilken form der kan klages,

			om konsekvenserne af at en klage ikke tages til følge mv.
2.3. De bindende virksomhedsregler skal være underlagt revision/tilsyn	Ja	Ja	Koncernen skal i de bindende virksomhedsregler forpligte sig til regelmæssigt at blive underlagt databeskyttelsesrevision/tilsyn. Revisionerne/tilsynene kan foretages af både interne og eksterne enheder. Ligeledes skal koncernen forpligte sig til at besvare spørgsmål fra f.eks. en intern databeskyttelsesrådgiver. Det skal fremgå af de bindende virksomhedsregler, at revisionen/tilsynet skal dække alle aspekter af reglerne. Herudover skal det fremgå, at resultaterne af revisionerne/tilsynene vil blive kommunikeret til koncernens databeskyttelsesrådgiver og til koncernens modervirksomheds bestyrelse. Endvidere skal det fremgå af de bindende virksomhedsregler, at kompetente tilsynsmyndigheder kan få adgang til resultaterne af revisionerne/tilsynene, og at tilsynsmyndighederne også kan foretage deres egne tilsyn. Ansøgningsblanketten skal indeholde en nærmere beskrivelse af revisions/tilsynssystemet.
2.4. Udpegelse af et netværk af databeskyttelsesrådgivere til at	Ja	Nej	Koncernen skal forpligte sig til at udpege et netværk af databeskyttelsesrådgivere, med støtte

håndtere klager og efterse iagttagelsen af reglerne.			fra koncernens topledelse, der kan sikre reglernes efterlevelse. Der bør, i de bindende virksomhedsregler, være en kort beskrivelse af den interne struktur og rollen og ansvaret for netværket af databeskyttelsesrådgivere.
3. Samarbejdsforpligtelse			
3.1. Forpligtelse til at samarbejde med tilsynsmyndigheder.	Ja	Ja	De bindende virksomhedsregler skal indeholde en klar forpligtelse for alle koncernvirksomheder til at samarbejde med tilsynsmyndighederne og lade sig blive underlagt revision/tilsyn af disse. Ligeledes skal koncernvirksomhederne efterleve eventuelle afgørelser fra tilsynsmyndighederne.
4. Beskrivelse af behandlinger og data flows			
4.1. Beskrivelse af de overførsler, der vil være omfattet af de bindende virksomhedsregler.	Ja	Ja	De bindende virksomhedsregler skal indeholde en general beskrivelse af, hvilke overførsler, der er omfattet af de bindende virksomhedsregler. Det bør bl.a. beskrives, hvilke typer af oplysninger, der overføres, hvad formålet med overførslerne er og hvilke dataeksportører og dataimportører, der er tale om.
4.2. En beskrivelse af den geografiske og materielle rækkevidde af de bindende virksomhedsregler (typen	Ja	Ja	Det bør af de bindende virksomhedsregler i forhold til den geografiske rækkevidde fremgå, om reglerne gælder for alle personoplysninger, der overføres fra

af oplysninger, typen af registrerede, hvilke lande mv.).			EU, eller om reglerne gælder for alle behandlinger af personoplysninger inden for koncernen, uanset hvorfra oplysningerne måtte stamme. For så vidt angår den materielle rækkevidde bør det fremgå, hvilke registrerede, der overføres oplysninger om (ansatte, kunder mv.).
5. Mekanisme til rapportering af ændringer			
5.1. Procedure for opdatering af reglerne.	Ja	Ja	De bindende virksomhedsregler skal indeholde en forpligtelse til, at koncernen rapporterer ændringer af reglerne til alle koncernvirksomheder og tilsynsmyndighederne. Opdatering af bindende virksomhedsregler, eller en liste over bundne koncernvirksomheder, kan ske uden at ansøge om ny tilladelse, hvis: i) En bestemt person fører en fuldt ud opdateret liste over medlemmer af koncernen samt over ændringer og informerer de registrerede eller tilsynsmyndighederne om ændringerne efter anmodning. ii) Der ikke overføres oplysninger til en ny koncernvirksomhed, før denne er effektivt bundet af de bindende virksomhedsregler. iii) Væsentlige ændringer én gang om året bliver rapporteret

			til de tilsynsmyndigheder, der har meddelt tilladelse. I rapporteringen bør ændringerne kort forklares.
6. Databeskyttelse			
6.1. Beskrivelse af databeskyttelsesprincipper, herunder i forhold til overførsler og videreoverførsler ud af EU.	Ja	Ja	De bindende virksomhedsregler bør forklare, hvordan de følgende principper bliver iagttaget: i) Transparens og rimelighed ii) Formålsbegrænsning. iii) Datakvalitet. iv) Datasikkerhed, herunder forpligtelsen til at indgå databehandleraftaler. v) Retten til indsigt, berigtigelse og indsigelse. vi) Begrænsning i overførsler og videreoverførsler til dataansvarlige og databehandlere, der ikke er en del af koncernen.
6.2. Liste over bundne koncernvirksomheder.	Nej	Ja	I ansøgningsblanketten skal der være en fuldstændig liste over de koncernvirksomheder, der er bundet af de bindende virksomhedsregler.
6.3. Hvis national lovgivning forhindrer en koncernvirksomhed i at efterleve reglerne.	Ja	Nej	De bindende virksomhedsregler skal indeholde en klar forpligtelse til, at en koncernvirksomhed skal underrette koncernens EU hovedkvarter, eller den EU koncernvirksomhed, der har accepteret ansvaret for at hæfte for brud på de bindende virksomhedsregler, hvis de finder, at de bliver underlagt lovgivning, der forhindrer dem i at efterleve reglerne.

			Samtidig bør de bindende virksomhedsregler indeholde en forpligtelse til, at koncernens EU hovedkvarter, eller den EU koncernvirksomhed, der har accepteret ansvaret for at hæfte for brud på de bindende virksomhedsregler, vil træffe en ansvarlig beslutning i forhold til hvad der skal ske, når der er en konflikt mellem nationale lovgivning i et tredjeland og de bindende virksomhedsregler. Den relevante koncernvirksomhed bør også konsultere den kompetente tilsynsmyndighed, hvis den er i tvivl.
6.4. En erklæring om forholdet mellem national lovgivning og de bindende virksomhedsregler.	Ikke et krav	Ikke et krav	Selvom det ikke er et krav, er det en fordel, hvis forholdet mellem de bindende virksomhedsregler og gældende lovgivning specificeres. De bindende virksomhedsregler kunne således f.eks. foreskrive, at når lokal lovgivning – herunder EU lovgivning – indebærer en bedre beskyttelse af personoplysninger end de bindende virksomhedsregler, da har denne lovgivning forrang. Personoplysninger skal under alle omstændigheder behandles i overensstemmelse med gældende lovgivning.

Bilag 5 – skema over indholdsmæssige minimumskrav til et sæt bindende virksomhedsregler for databehandlere

Skemaet er baseret på Artikel 29-gruppens udtalelse i WP 195. Bemærk venligst, at nedenstående ikke er en 1:1 oversættelse af den officielle engelske version. En koncern, der ønsker at udarbejde et sæt bindende virksomhedsregler, bør derfor også læse den officielle tekst.

Indholdsmæssige minimumskrav	I de bindende virksomhedsregler	I ansøgningsblanketten	Bemærkninger
1. Bindende virkning			
Internt i koncernen			
1.1. Forpligtelse til at respektere de bindende virksomhedsregler	Ja	Ja	De bindende virksomhedsregler skal indeholde en klar forpligtelse for alle koncernvirksomheder og for alle ansatte til at respektere de bindende virksomhedsregler. Endvidere skal de bindende udtrykkeligt fastslå, at alle koncernvirksomheder og alle ansatte skal respektere den instruktion, der fremgår af databehandleraftalen med den dataansvarlige.
1.2. En redegørelse for hvordan reglerne er gjort bindende for koncernvirksomhederne og de ansatte	Nej	Ja	I forhold til koncernvirksomhederne kan reglerne f.eks. være blevet gjort bindende ved aftaler mellem koncernvirksomhederne eller ved hjælp af ensidige erklæringer fra "modervirksomheden". I forhold til de ansatte kan reglerne f.eks. være blevet gjort bindende via tillæg til ansættel-

			seskontrakter eller via interne politikker udstykket af ledelsen. Manglende iagttagelse skal være sanktioneret.
Eksternt			
1.3. Fastsættelse af tredjepartsrettigheder for de registrerede, herunder retten til at klage til en relevant tilsynsmyndighed eller indbringe en klage for domstolene (kan vælge mellem jurisdiktionen for EU dataeksportøren eller jurisdiktionen for koncernens EU hovedkvarter).	Ja	Ja	De bindende virksomhedsregler skal give de registrerede ret til at håndhæve de bindende virksomhedsregler som tredjepartsbegunstigede, hvis de registrerede ikke kan gøre deres krav gældende overfor den dataansvarlige, fordi denne er faktisk forsvundet eller er ophørt med at eksistere eller lignende. Dette forudsætter, at der ikke er trådt en ny dataansvarlig i den dataansvarliges sted. De bindende virksomhedsregler skal give de registrerede mulighed for at håndhæve alle tredjepartsrettighederne, herunder retten til at modtage erstatning. De registrerede skal også kunne indbringe en klage for de kompetente tilsynsmyndigheder eller domstole i den EU dataansvarliges jurisdiktion. Er dette ikke muligt – f.eks. hvis den dataansvarlige er ophørt med at eksistere – kan de registrerede indbringe deres klage for de kompetente tilsynsmyndigheder eller domstole i den jurisdiktion, hvor EU dataeksportøren er hjemhørende, i den jurisdiktion hvor

			databehandlerens EU hovedkvarter er hjemhørende eller i den jurisdiktion hvor den EU koncernvirksomhed, der har påtaget sig ansvaret er hjemhørende. Er ingen af disse jurisdiktioner en mulighed, kan de registrerede indbringe deres klage for de kompetente tilsynsmyndigheder eller domstole i den pågældendes egen jurisdiktion. Den registreredes tredjepartsrettigheder skal dække punkt 1.1., 1.3., 1.5., 1.7., 1.8., 2.2., 3.1., 3.2., 6.1., 6.2. og 6.3. i dette skema.
1.4. Ansvar i forhold til de dataansvarlige.	Ja	Ja	De bindende virksomhedsregler skal gøres bindende i forhold til den dataansvarlige gennem en specifik henvisning i databehandleraftalen. Herudover skal det fremgå af de bindende virksomhedsregler, at alle dataansvarlige skal have ret til at håndhæve reglerne imod enhver koncernvirksomhed, der har forbrudt sig mod disse. De dataansvarliges rettigheder skal inkludere juridiske retsmidler og retten til at modtage erstatning.
1.5. Koncernen accepterer at hæfte for at betale erstatning og for at afhjælpe brud på	Ja	Ja	I de bindende virksomhedsregler skal koncernens EU hovedkvarter, den EU koncernvirksomhed, der har accepteret ansvaret eller

reglerne.			EU dataeksportørkoncernvirksomheden forpligtes til at hæfte for brud på de bindende virksomhedsregler begået af koncernvirksomheder i tredjelande. De skal endvidere forpligtes til at afhjælpe brud på reglerne samt til at betale erstatning for eventuelle tab lidt som følge af bruddet på reglerne. Ovennævnte koncernvirksomheder skal acceptere ansvaret, som var bruddet på reglerne sket i deres egen jurisdiktion. Ansvaret kan endvidere ikke flyttes over på en underdatabehandler. Hvis ingen koncernvirksomheder er etableret i EU, skal moderkoncernvirksomheden acceptere ansvaret. I disse situationer skal de registrerede og de dataansvarlige kunne indbringe en klage for en tilsynsmyndighed eller domstol i sin egen jurisdiktion.
1.6. Koncernen har de fornødne aktiver	Nej	Ja	I ansøgningsblanketten skal det bekræftes, at den EU koncernvirksomhed, der har accepteret at hæfte for brud på reglerne uden for EU, har de fornødne aktiver til at betale eventuel erstatning mv.
1.7. Koncernen har bevisbyrden	Ja	Ja	Det skal fremgå af de bindende virksomhedsregler, at når en registreret eller en dataansvarlig kan demonstrere, at de har lidt et

			tab, og når de kan sandsynliggøre, at tabet hidrører fra et brud på de bindende virksomhedsregler, da har den EU koncernvirksomhed, der har accepteret at hæfte for brud på reglerne uden for EU, bevisbyrden for, at en koncernvirksomhed uden for EU ikke er ansvarlig for et brud på reglerne, som har resulteret i, at en registreret søger erstatning. Kan det dokumenteres, at en koncernvirksomhed uden for EU ikke er ansvarlig for et brud, kan den EU koncernvirksomhed, der har accepteret at hæfte for eventuelle brud, også frasige sig ansvaret.
1.8. De registrerede har let adgang til de bindende virksomhedsregler, herunder især information om de registreredes tredjepartsrettigheder, og hvordan de kan påberåbe sig dem.	Ja	Nej	Adgang for den dataansvarlige: Databehandleraftalen mellem den dataansvarlige og databehandlerkoncernen vil sikre, at de bindende virksomhedsregler er en del af kontrakten. De bindende virksomhedsregler vil således være vedlagt databehandleraftalen som et anneks. Alternativt vil der, i databehandleraftalen, blive henvist til de bindende virksomhedsregler og hvortil reglerne kan findes elektronisk. Adgang for de registrerede: De bindende virksomhedsregler skal offentliggøres på koncernens hjemmeside og være let

			tilgængelig. Alternativt kan koncernen nøjes med at offentliggøre et dokument med information om punkt 1.1., 1.3., 1.4., 1.6., 1.7., 2.2., 3.1., 3.2., 6.1., 6.2. og 6.3. i dette skema.
2. Efterlevelse			
2.1. Der skal være et passende uddannelsesprogram	Ja	Ja	Det skal fremgå af de bindende virksomhedsregler, at ansatte, der permanent eller regelmæssigt behandler personoplysninger, vil skulle gennemgå et passende uddannelsesprogram i forhold til de bindende virksomhedsregler. Typisk vil det være en fordel at vedlægge eksempler på, hvordan de ansatte vil modtage den fornødne uddannelse.
2.2. Der skal være en klagebehandlingsprocedure	Ja	Ja	De bindende virksomhedsregler skal indeholde en forpligtelse til, at databehandlerkoncernen opretter et specifikt kontaktpunkt for de registrerede. Alle medlemmer af koncernen skal have pligt til – uden unødig forsinkelse – at videresende et krav eller ønske fra en registreret til den dataansvarlige. Koncernvirksomhederne har ikke pligt til at behandle den registreredes krav eller ønske, med mindre dette er aftalt med den dataansvarlige. De bindende virksomhedsregler

			skal indeholde en forpligtelse til, at databehandlerkoncernen behandler klager mv. fra de registrerede, hvis den dataansvarlige f.eks. er ophørt med at eksistere. I de situationer, hvor databehandlerkoncernen behandler klager, da skal disse håndteres af en nem identificerbar afdeling eller person, som har den fornødne uafhængighed fra resten af koncernen.
2.3. De bindende virksomhedsregler skal være underlagt revision/tilsyn	Ja	Ja	Koncernen skal i de bindende virksomhedsregler forpligte sig til regelmæssigt at blive underlagt databeskyttelsesrevision/tilsyn. Revisionerne/tilsynene kan foretages af både interne og eksterne enheder. Ligeledes skal koncernen forpligte sig til at besvare spørgsmål fra f.eks. en intern databeskyttelsesrådgiver. Det skal fremgå af de bindende virksomhedsregler, at revisionen/tilsynet skal dække alle aspekter af reglerne. Herudover skal det fremgå, at resultaterne af revisionerne/tilsynene vil blive kommunikeret til koncernens databeskyttelsesrådgiver og til koncernens modervirksomheds bestyrelse, ligesom resultaterne skal gøres tilgængelige for den dataansvarlige. Endvidere skal det fremgå af de

			bindende virksomhedsregler, at de tilsynsmyndigheder, der er kompetente i forhold til den dataansvarlige kan få adgang til resultaterne af revisionerne/tilsynene, og at tilsynsmyndighederne også kan foretage deres egne tilsyn. Alle koncernvirksomheder og eventuelle underdatabehandlere skal acceptere, at en dataansvarlig kan føre revision/tilsyn med behandlinger, der relaterer sig til den pågældende dataansvarlige. Revisionerne/tilsynene kan udføres af den dataansvarlige selv eller en repræsentant for denne. Ansøgningsblanketten skal indeholde en nærmere beskrivelse af revisions/tilsynssystemet.
2.4. Udpegelse af et netværk af databeskyttelsesrådgivere til at håndtere klager og efterse iagttagelsen af reglerne.	Ja	Nej	Koncernen skal forpligte sig til at udpege et netværk af databeskyttelsesrådgivere, med støtte fra koncernens topledelse, der kan sikre reglernes efterlevelse. Der bør, i de bindende virksomhedsregler, være en kort beskrivelse af den interne struktur og rollen og ansvaret for netværket af databeskyttelsesrådgivere.
3. Samarbejdsforpligtelse			
3.1. Forpligtelse til at samarbejde med til-	Ja	Ja	De bindende virksomhedsregler skal indeholde en klar forpligtel-

synsmyndigheder.			se for alle koncernvirksomheder til at samarbejde med tilsynsmyndighederne og lade sig blive underlagt revision/tilsyn af disse. Ligeledes skal koncernvirksomhederne efterleve eventuelle afgørelser fra tilsynsmyndighederne.
3.2. Forpligtelse til at samarbejde med den dataansvarlige.	Ja	Ja	De bindende virksomhedsregler skal indeholde en klar forpligtelse for alle koncern databehandlere og underdatabehandlere til at samarbejde med og assistere den dataansvarlige med at overholde gældende databeskyttelsesregler. Ovennævnte skal ske inden for rimelig tid og i et rimeligt omfang.
4. Beskrivelse af behandlinger og data flows			
4.1. Beskrivelse af de overførsler, der vil være omfattet af de bindende virksomhedsregler samt reglernes materielle rækkevidde.	Ja	Ja	De bindende virksomhedsregler skal indeholde en liste med de koncernvirksomheder, der er omfattet af reglerne. Den koncernvirksomhed, der indgiver ansøgningen om godkendelse af reglerne skal overfor tilsynsmyndigheden give en generel beskrivelse af reglernes materielle rækkevidde (typer af oplysninger, formål med overførslerne samt dataeksportører og dataimportører i og uden for EU).
4.2. Erklæring om den geografiske rækkevid-	Ja	Ja	Det bør af de bindende virksomhedsregler fremgå, at det er op

de.			til den dataansvarlige at beslutte, om de bindende virksomhedsregler alene skal gælde i forhold til personoplysninger, der behandles med databehandlingsformål og som er underlagt EU lovgivning, *eller* for al databehandling uanset hvorfra personoplysningerne måtte stamme.
5. Mekanisme til rapportering af ændringer			
5.1. Procedure for opdatering af reglerne.	Ja	Ja	De bindende virksomhedsregler skal indeholde en forpligtelse til, at koncernen rapporterer ændringer af reglerne til alle koncernvirksomheder, til tilsynsmyndighederne og til den dataansvarlige. Hvis en ændring påvirker behandlingsbetingelserne, skal den dataansvarlige underrettes i så god tid, at den pågældende har mulighed for at protestere mod ændringen eller hæve kontrakten, inden ændringen træder i kraft. Opdatering af bindende virksomhedsregler, eller en liste over bundne koncernvirksomheder, kan ske uden at ansøge om ny tilladelse, hvis: i) En bestemt person fører en fuldt ud opdateret liste over medlemmer af databehandler-

			koncernen og underdatabehandlere og informerer den dataansvarlige, de registrerede og tilsynsmyndighederne om ændringerne. ii) Samme person fører en liste over ændringer i de bindende virksomhedsregler og giver systematisk nødvendige informationer herom til den dataansvarlige og til tilsynsmyndighederne efter anmodning. iii) Der ikke overføres oplysninger til en ny koncernvirksomhed, før denne er effektivt bundet af de bindende virksomhedsregler. iv) Væsentlige ændringer én gang om året bliver rapporteret til de tilsynsmyndigheder, der har meddelt tilladelse. I rapporteringen bør ændringerne kort forklares.
6. Databeskyttelse			
6.1. Beskrivelse af databeskyttelsesprincipper, herunder i forhold til overførsler og videreoverførsler ud af EU.	Ja	Ja	De bindende virksomhedsregler skal indeholde følgende principper: i) Transparens og rimelighed (databehandlere og underdatabehandlere har en generel forpligtelse til at hjælpe den dataansvarlige med at leve op til sine forpligtelser). ii) Formålsbegrænsning (forpligtelse til alene at behandle oplysninger på vegne af den dataansvarlige og efter dennes instruks samt pligt til at tilbagelevere

			oplysninger eller slette ved aftales ophør). iii) Datakvalitet (forpligtelse til at hjælpe den dataansvarlige med at leve op til sine forpligtelser).. iv) Datasikkerhed (databehandlere og underdatabehandlere skal som minimum have en sikkerhed, der lever op til de krav, som følger af den nationale lovgivning, der gælder for den dataansvarlige. Databehandlere og underdatabehandlere skal også straks underrette den dataansvarlige om eventuelle sikkerhedsbrister.). v) Rettigheder for de registrerede (databehandlere og underdatabehandlere skal på anmodning fra den dataansvarlige hjælpe med at sikre, at de registreredes rettigheder bliver iagttaget). vi) Underdatabehandling inden for koncernen (kræver forudgående orientering af og skriftligt samtykke fra den dataansvarlige. Et sådant samtykke kan efter aftale gives generelt). vii) Videreoverførsler til eksterne underdatabehandlere (kræver forudgående orientering af og skriftlige samtykke fra den dataansvarlige. Et samtykke kan også her gives generelt. Det er en forudsætning, at der er et overførselsgrundlag (f.eks. Kommissionens standardkon-

			traktbestemmelser), og at det sikres, at underdatabehandleren skal leve op til de samme krav, som databehandleren er underlagt i den oprindelige databehandleraftale.).
6.2. Liste over bundne koncernvirksomheder.	Ja	Ja	I ansøgningsblanketten skal der være en fuldstændig liste over de koncernvirksomheder, der er bundet af de bindende virksomhedsregler.
6.3. Hvis national lovgivning forhindrer en koncernvirksomhed i at efterleve reglerne.	Ja	Nej	De bindende virksomhedsregler skal indeholde en klar forpligtelse til, at en koncernvirksomhed hurtigt skal underrette den dataansvarlige; koncernens EU hovedkvarter; den EU koncernvirksomhed, der har accepteret ansvaret for at hæfte for brud på de bindende virksomhedsregler samt den kompetente tilsynsmyndighed i den dataansvarliges jurisdiktion, hvis de finder, at de er eller vil blive underlagt lovgivning, der forhindrer dem i at efterleve de bindende virksomhedsregler eller databehandleraftalen. I sådan tilfælde kan den dataansvarlige suspendere overførslerne og/eller hæve kontrakten. Alle juridisk bindende anmodninger om udlevering af personoplysninger fra en retshåndhævelsesmyndighed skal kommunikeres til den dataansvarlige,

			med mindre dette ikke er muligt som følge af et lovbestemt forbud imod dette. Under alle omstændigheder bør anmodningen sættes i bero, indtil den kompetente tilsynsmyndighed i den dataansvarliges jurisdiktion og den kompetente tilsynsmyndighed i koncernens EU hovedkvarter er blevet underrettet.
6.4. En erklæring om forholdet mellem national lovgivning og de bindende virksomhedsregler.	Ja	Nej	De bindende virksomhedsregler skal specificere forholdet mellem de bindende virksomhedsregler og relevant gældende lovgivning. Af de bindende virksomhedsregler skal det fremgå, at når lokal lovgivning – herunder EU lovgivning – indebærer en bedre beskyttelse af personoplysninger end de bindende virksomhedsregler, da har denne lovgivning forrang. Personoplysninger skal i alle tilfælde behandles i overensstemmelse med gældende lovgivning.

6.5. Overførsel uden hjemmel i EU-retten, artikel 48

6.5.1. Præsentation

Med databeskyttelsesforordningens artikel 48 fastlås det, at domme og afgørelser fra domstole og myndigheder i tredjelande kun kan begrunde en overførsel eller videregivelse af personoplysninger til det pågældende tredjeland, hvis de bygger på en international aftale mellem det anmodende tredjeland og EU eller en medlemsstat.

I modsætning til de øvrige bestemmelser i databeskyttelsesforordningens kapitel V, om overførsel af personoplysninger til tredjelande eller internationale organisationer, gælder artikel 48 for både *overførsel* og *videregivelse* af personoplysninger til tredjelande. Artikel 48 skal således ikke kun iagttages i forhold til vurderingen af, hvorvidt der er hjemmel til overførslen i forordningens kapitel V, men også i forhold til, om der er hjemmel til selve videregivelsen i behandlingsreglerne i forordningens kapitel II.

6.5.2. Gældende ret

Databeskyttelsesdirektivet og persondataloven indeholder ikke regler, der svarer til bestemmelsen i databeskyttelsesforordningens artikel 48.

Efter persondatalovens § 27, stk. 3, nr. 4, (databeskyttelsesdirektivets artikel 26, stk. 1, litra d), kan der bl.a. ske overførsel, hvis dette er nødvendigt for, at et retskrav kan fastlægges, gøres gældende eller forsvares.[720] Dette vil bl.a. kunne være aktuelt i forbindelse med internationale tvister og retssager. I forlængelse heraf nævnes det, at et særligt spørgsmål, der ikke er taget stilling til i forarbejderne til persondataloven, er, om et retskrav kan have sit grundlag i et tredjelands lovgivning.

Der er ifølge kommentaren tale om et vanskeligt spørgsmål, som næppe kan besvares entydigt. I kommentaren henvises i den forbindelse bl.a. til bogen "Retlig regulering af internationale persondataoverførsler",[721] hvor spørgsmålet er behandlet, og hvor det forsigtigt konkluderes, at det ikke kan udelukkes, at fremmed ret, herunder tredjelands ret, i sig selv kan udgøre overførselsgrundlaget, samtidig med, at der peges på, at det i Datatilsynets aktuelle praksis (som omtales) antages, at fremmed ret ikke kan begrunde en overførsel af oplysninger.

Der kan i den forbindelse henvises til Justitsministeriets besvarelse af 23. maj 2012 af spørgsmål nr. 700 (Alm. del) fra Folketingets Retsudvalg, hvoraf det bl.a. fremgår, at virk-

[720] Persondataloven med kommentarer (2015), s. 453.
[721] Peter Blume, Retlig regulering af internationale persondataoverførsler, 1. udgave (2006), s. 101-104.

somheder i Danmark, efter Datatilsynets vurdering, kun vil kunne udlevere personoplysninger til amerikanske myndigheder, hvis de er berettigede dertil efter reglerne i persondataloven, eller hvis de har en pligt dertil efter anden lovgivning, der gælder i Danmark. Datatilsynet vurderer umiddelbart, at et krav om udlevering til amerikanske myndigheder begrundet i US Patriot Act ikke i sig selv indebærer en hjemmel til udlevering efter persondataloven, og at hvis der ikke foreligger hjemmel i dansk lovgivning til udleveringen, herunder eventuelt en retskendelse, kan en dansk databehandlers udlevering af oplysninger efter omstændighederne, udgøre en overtrædelse af persondataloven.

6.5.2.1. Udtalelse fra Kommissionen af 23. august 2011

Kommissionen har i et svar af 23. august 2011 på et spørgsmål fra Europa-Parlamentet om håndhævelse af reglerne i den amerikanske Patriot Act over for enheder etableret i EU udtalt følgende:

> "The United States (US) Patriot Act of 2001 establishes a wide range of measures for US competent authorities in the fight against terrorist acts. Amongst other things, the US Patriot Act gives US law enforcement and intelligence agencies greater powers to access personal data and to engage in surveillance activities. In this regard, measures such as a court order from the Foreign Intelligence Surveillance Court for production of information (provided in Section 215) or a "national security letter" issued by the Federal Bureau of Investigation (FBI) (provided in Section 505) can be issued upon a US established legal entity. A legal entity established under US law is subject to US law, including such court orders or 'national security letters' that might request production of information or evidence on specific persons or facts related to a particular counterterrorism investigation.
>
> However, in accordance with international public law, and in the absence of a recognised jurisdictional link, a foreign law or statute cannot directly impose legal obligations on organisations or undertakings established in a third country regarding the activities performed within the territory of that third country. In order to give effect to the different legal obligations provided by the US Patriot Act on legal entities established in the EU, it would be necessary that they are imposed by an EU legal instrument or a Member State's legal instrument which respects its obligations under EC law, including data protection principles.

> The Commission attaches the utmost importance to the fundamental rights to freedom of expression, respect for private and family life and personal data protection, which are applied in the EU without discrimination on the basis of nationality, citizenship or place of residence.
>
> *The Commission's upcoming proposals for reform of the EU data protection framework will therefore particularly focus on the challenges posed by globalisation and modern technologies.*" [kursivering foretaget her]

Af Kommissionens udtalelse må det således bl.a. udledes, at lovgivning mv. i et tredjeland ikke kan forpligte en organisation eller virksomhed i EU. Dette kan kun ske, hvis der foreligger en anerkendt aftale[722], der foreskriver noget andet, og hvis organisationen eller virksomheden i øvrigt iagttager de forpligtelser, som er pålagt i medfør af EU- og/eller medlemsstatslovgivning, herunder databeskyttelseslovgivning.

6.5.2.2. Udtalelser fra Artikel 29-gruppen af 25. november 2005 og 11. februar 2009

6.5.2.2.1. Udtalelsen af 25. november 2005

I en udtalelse af 25. november 2005 om en ensartet fortolkning af databeskyttelsesdirektivets artikel 26, stk. 1 (WP 114), har Artikel 29-gruppen bl.a. på side 15 ff. udtalt sig om bestemmelsen i direktivets artikel 26, stk. 1, litra d.

Om muligheden for at anvende artikel 26, stk. 1, litra d, som overførselsgrundlag, når myndigheder i tredjelande kræver oplysninger udleveret fra dataansvarlige i EU, udtaler Artikel 29-gruppen bl.a., at man ved udarbejdelsen af direktivet helt klart har taget udgangspunkt i, at kun vigtige samfundsinteresser, der identificeres som sådan i henhold til den nationale lovgivning, som finder anvendelse på dataansvarlige i EU, kan udgøre de vigtige samfundsinteresser, der henvises til i bestemmelsen. Artikel 29-gruppen udtaler endvidere, at enhver anden tolkning ville gøre det for nemt for et tredjelands myndigheder at omgå kravet om tilstrækkelig beskyttelse i modtagerlandet som fastsat i databeskyttelsesdirektivet.

Det er således en forudsætning for en overførsel efter bestemmelsen, at overførslen også er af interesse for myndighederne i en EU-medlemsstat. Dette kan f.eks. være tilfældet, hvis overførslen sker i overensstemmelse med en international aftale, som både den pågældende EU-medlemsstat og tredjelandet har ratificeret.

[722] F.eks. Haagerkonventionen af 18. marts 1970 om bevisoptagelse i udlandet i sager om civile eller kommercielle spørgsmål og Haagerkonventionen af 25. oktober 1980 om international retshjælp.

6.5.2.2.2. Udtalelsen af 11. februar 2009

Artikel 29-gruppen har endvidere i en udtalelse af 11. februar 2009 om såkaldt "pre-trial discovery"[723] i forbindelse med grænseoverskridende civile retssager (WP 158) udtalt, at overførsel af personoplysninger fra en EU-medlemsstat til et tredjeland i forbindelse med pre-trial discovery kræver, at to betingelser er opfyldt.

For det første skal selve videregivelsen af oplysningerne have hjemmel i behandlingsreglerne i databeskyttelsesdirektivets artikel 7 m.fl., og for det andet skal selve overførslen have hjemmel i direktivets artikel 26 m.fl. Der gælder således et "dobbelt hjemmelskrav".

Med hensyn til hjemlen til videregivelse udtaler Artikel 29-gruppen i forhold til direktivets artikel 7, litra c – hvorefter der kan behandles oplysninger, hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, som gælder for den dataansvarlige – at en retlig forpligtelse, der hidrører fra et tredjeland ikke kan udgøre en retlig forpligtelse i bestemmelsens forstand.

Artikel 29-gruppen udtaler endvidere, at en retlig forpligtelse kan følge af, at de enkelte medlemsstater har tilsluttet sig f.eks. ovenfornævnte Haagerkonventioner.

For så vidt angår overførselsdelen udtaler Artikel 29-gruppen, at en overførsel til et tredjeland skal have hjemmel i databeskyttelsesdirektivets artikel 25 eller 26.

En hjemmel kunne i den forbindelse være direktivets artikel 26, stk. 1, litra d, som Artikel 29-gruppen har udtalt sig om i WP 114, jf. ovenfor.

6.5.3. Databeskyttelsesforordningen

Det fremgår af databeskyttelsesforordningens artikel 48, at enhver dom afsagt af en domstol eller ret og enhver afgørelse truffet af en administrativ myndighed i et tredjeland, der kræver, at en dataansvarlig eller en databehandler overfører eller videregiver personoplysninger, kun kan anerkendes eller håndhæves på nogen måde, hvis den bygger på en international aftale, såsom en traktat om gensidig retshjælp mellem det anmodende tredjeland og Unionen eller en medlemsstat, uden at det berører andre grunde til overførsel i henhold til dette kapitel.

Af præambelbetragtning nr. 115 fremgår det, at visse tredjelande vedtager love, forskrifter og andre retsakter med det formål direkte at regulere behandlingsaktiviteter udøvet af fysiske og juridiske personer under medlemsstaternes jurisdiktion. Som eksempler på sådanne

[723] Pre-trial discovery er den forberedende fase umiddelbart inden domsforhandlingen, hvor parterne hver især ved en discovery order pålægges at fremlægge, hvad de har af relevant materiale i sagen.

retsakter fremgår det endvidere, at disse kan omfatte retsafgørelser eller administrative myndigheders afgørelser i tredjelande, der kræver, at en dataansvarlig eller en databehandler overfører personoplysninger, og som ikke er baseret på en gældende international aftale som en traktat om gensidig retshjælp mellem det anmodende tredjeland og Unionen eller en medlemsstat. Om ekstraterritorial anvendelse af sådanne love, forskrifter og andre retsakter fremgår det, at disse kan være i strid med folkeretten og hindre opnåelse af den beskyttelse af fysiske personer, der sikres i Unionen ved denne forordning. Herudover fremgår det om muligheden for at overføre oplysninger, at dette kun bør tillades, hvis denne forordnings betingelser for overførsel til tredjelande er opfyldt. Endelig fremgår det, at forordningens betingelser bl.a. kan være opfyldt, hvis videregivelse er nødvendig af hensyn til vigtige samfundsinteresser, der anerkendes i EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er omfattet af.

Databeskyttelsesforordningens artikel 48 synes umiddelbart at være udtryk for en slags kodificering af allerede kendte synspunkter om emnet fra Kommissionen og Artikel 29-gruppen, jf. ovenfor.

Når det sidst i artikel 48 fremgår, at bestemmelsen ikke berører andre grunde til overførsel i henhold til dette kapitel, skyldes dette formentlig, at man primært har et ønske om at begrænse overførsler til tredjelande baseret på undtagelserne i forordningens artikel 49, stk. 1, litra d og e, som artikel 48 hovedsagligt må antages at få betydning for i praksis. Af artikel 49, stk. 4, fremgår det således også, at de samfundsinteresser, der er omhandlet i artikel 49, stk. 1, litra d, skal være anerkendt i EU-retten eller retten i den medlemsstat, som den dataansvarlige er underlagt.

Hvis overførslerne sker på grundlag af de øvrige bestemmelser i databeskyttelsesforordningens kapitel V (artikel 45, 46 og 47), vil der – i modsætning til, når undtagelserne i artikel 49 bliver anvendt – være sikkerhed for, at modtageren i et tredjeland er underlagt en række databeskyttelsesretlige principper mv., der sikrer et tilstrækkeligt beskyttelsesniveau i forhold til de registreredes rettigheder.

6.5.4. Overvejelser

Der er tale om en ny regel sammenholdt med databeskyttelsesdirektivet og persondataloven. Bestemmelsen synes umiddelbart at være udtryk for en slags kodificering af allerede kendte synspunkter om emnet fra bl.a. Kommissionen og Artikel 29-gruppen.

6.6. Undtagelser i særlige situationer, artikel 49

6.6.1. Præsentation

I databeskyttelsesforordningens artikel 49 fastsættes der regler om, at der i særlige situationer kan ske overførsel af personoplysninger til tredjelande, der ikke har et tilstrækkeligt beskyttelsesniveau, som omtalt i artikel 45, og hvor der heller ikke i medfør af artikel 46 er givet fornødne garantier i forbindelse med overførslen.

De fleste af reglerne i artikel 49 er kendt fra databeskyttelsesdirektivet og persondataloven, men bestemmelsen indeholder enkelte nyskabelser.

6.6.2. Gældende ret

I persondatalovens § 27, stk. 3, nr. 1-8, oplistes der en række situationer, hvor der kan ske overførsel af personoplysninger til et tredjeland, som ikke sikrer et tilstrækkeligt beskyttelsesniveau, jf. § 27, stk. 1.

Bestemmelserne i persondatalovens § 27, stk. 3, nr. 1-6, har baggrund i databeskyttelsesdirektivets artikel 26, stk. 1, hvorimod nr. 7-8, der falder uden for databeskyttelsesdirektivets anvendelsesområde, er medtaget af informative grunde.[724]

6.6.2.1. Generelt om muligheden for at anvende § 27, stk. 3, som overførselsgrundlag

Artikel 29-gruppen har i en udtalelse af 25. november 2005 udtalt sig om en ensartet fortolkning af databeskyttelsesdirektivets artikel 26, stk. 1 (WP 114).

På side 6 ff. udtaler Artikel 29-gruppen bl.a. om betydningen af artikel 26, stk. 1, i forhold til direktivet som helhed, at direktivet virker en smule paradoksalt, når alle disse forskellige regler om overførsel af personoplysninger sammenholdes, og det kan let give anledning til misforståelser. Artikel 29-gruppen anfører endvidere, at på den ene side har en række bestemmelser, nemlig bestemmelserne i artikel 25, stk. 1 og 6, samt artikel 26, stk. 2, til formål at sikre, at de personoplysninger, der overføres, fortsat er omfattet af en tilstrækkelig beskyttelse efter overførslen til modtagerlandet. Disse overførsler kan, ifølge Artikel 29-gruppen, finde sted, enten fordi lovgivningen i det pågældende tredjeland sikrer en tilstrækkelig beskyttelse, eller fordi der opnås en tilstrækkelig beskyttelse gennem standardkontraktbestemmelser eller andre passende foranstaltninger, herunder indgåelse af en kontrakt, vedtagelsen af bindende virksomhedsregler, selvcertificering med hensyn til over-

[724] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 27, stk. 3, nr. 7 og 8.

holdelsen af Safe Harbor-principperne[725] osv. Hertil kommer ifølge Artikel 29-gruppen, at en række nationale lovgivninger som nævnt ovenfor indeholder bestemmelser om, at der for visse overførsler skal foreligge en godkendelse eller en udtalelse fra de relevante nationale myndigheder (oftest de nationale databeskyttelsesmyndigheder).

Artikel 29-gruppen udtaler endvidere, at der på den anden side er en række bestemmelser, herunder artikel 26, stk. 1, der gør det betydeligt nemmere at overføre personoplysninger til et tredjeland. I medfør af disse bestemmelser skal den dataansvarlige, der tager initiativ til overførslen, ifølge Artikel 29-gruppen, hverken sikre sig, at modtageren sikrer en tilstrækkelig beskyttelse, eller anmode om en forudgående tilladelse[726] til overførslen fra de relevante myndigheder, såfremt en sådan procedure måtte finde anvendelse. Disse bestemmelser pålægger desuden, ifølge Artikel 29-gruppen, ikke modtageren at opfylde kravene i direktivet med hensyn til enhver behandling af oplysningerne i sit eget land (f.eks. principperne om formål, sikkerhed, indsigt osv.).

Ifølge Artikel 29-gruppen kan direktivets ordlyd umiddelbart føre til den konklusion, at de forskellige bestemmelser om overførsel af personoplysninger til tredjelande er modstridende. Artikel 29-gruppen udtaler endvidere, at formålet med princippet om tilstrækkelig beskyttelse som foreskrevet i artikel 25 er, når alt kommer til alt, at sikre, at fysiske personer, hvis personoplysninger overføres til et tredjeland, bevarer de grundlæggende rettigheder og frihedsrettigheder, som de har i forbindelse med behandlingen af disse oplysninger i EU. Det har også til formål at forhindre, at man blot ved at overføre oplysningerne til et tredjeland omgår den beskyttelse, som EU-lovgivningen om beskyttelse af personoplysninger giver.

Denne tilsyneladende dobbelthed i de principper, der er fastlagt i direktivet, afspejler, ifølge Artikel 29-gruppen, den kendsgerning, at udbygningen af den internationale samhandel i forskellige situationer kræver en vis fleksibilitet i de internationale dataoverførsler, herunder overførsel af personoplysninger (jf. direktivets betragtning 56).

En anden forklaring for denne tilsyneladende manglende konsistens er, ifølge Artikel 29-gruppen, at artikel 26, stk. 1, var udformet til at regulere et begrænset antal situationer, hvor det blev anset for passende at undtage fra kravet om tilstrækkelig beskyttelse i forbindelse med overførsler til tredjelande. Som gruppen allerede gjorde opmærksom på i ar-

[725] Safe Harbor-principperne er siden Artikel 29-gruppens udtalelse fra 2005 blevet erstattet af EU-U.S. Privacy Shield. Se mere herom i afsnit 6.2. om overførsel baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, artikel 45.

[726] I Danmark skal der i visse situationer indhentes en forudgående tilladelse efter persondatalovens § 50, stk. 2, når der f.eks. overføres følsomme personoplysninger til et tredjeland i medfør af lovens § 27, stk. 3, nr. 2-4.

bejdsdokument WP 12: "Disse undtagelser, som er trukket skarpt op, drejer sig for størstedelens vedkommende om tilfælde, hvor risiciene for de registrerede er forholdsvis begrænsede, og hvor andre interesser (samfundsmæssige interesser eller den registreredes egne interesser) går forud for den registreredes ret til privatlivets fred. Som undtagelser fra et generelt princip skal de fortolkes restriktivt. Desuden har medlemsstaterne lov til i den nationale lovgivning at fastsætte, at undtagelserne ikke skal gælde i bestemte tilfælde. Dette kunne f.eks. være tilfældet, hvor det er nødvendigt at beskytte særligt udsatte persongrupper, f.eks. arbejdstagere eller patienter."

Ifølge Artikel 29-gruppen har der blandt dataansvarlige imidlertid i praksis været tendens til at anvende disse undtagelser som en første valgmulighed, selv i situationer, hvor det ikke er relevant. Artikel 29-gruppen vil derfor gerne først og fremmest sikre, at alle berørte parter forstår, hvad der er anvendelsesområdet for og meningen med artikel 26, stk. 1, for at undgå, at de dataansvarlige anvender undtagelserne i de forkerte situationer. Dette kræver en entydig og fælles fortolkning af artikel 26, stk. 1, som sådan og af bestemmelsens rolle i forhold til direktivet som helhed.

Artikel 29-gruppen udtaler, at der i denne forbindelse skal tages udgangspunkt i den regel, som gruppen tidligere har henvist til i ovennævnte arbejdsdokument WP 12, nemlig at artikel 26, stk. 1, nødvendigvis skal fortolkes restriktivt.

Efter ovennævnte gennemgang af betydningen af artikel 26, stk. 1, i forhold til direktivet som helhed, kommer Artikel 29-gruppen på side 9 ff. med nogle generelle anbefalinger om anvendelsen af bestemmelsen.

Artikel 29-gruppen udtaler i den forbindelse bl.a., at den bedste praksis for en dataansvarlig, der ønsker at foretage en international dataoverførsel, således først er at undersøge, om det pågældende tredjeland yder en tilstrækkelig databeskyttelse, og herefter selv at sørge for, at de overførte oplysninger beskyttes i dette land. Den dataeksporterende dataansvarlige kan ved overførsel til USA opfordre dataimportøren til at tilslutte sig Safe Harbor-principperne.[727] Hvis databeskyttelsesniveauet i tredjelandet på grundlag af samtlige de forhold, der har indflydelse på overførslen, ikke vurderes at være tilstrækkeligt, bør den dataansvarlige, ifølge Artikel 29-gruppen, tage artikel 26, stk. 2, i betragtning, for således at opnå en tilstrækkelig beskyttelse ved f.eks. at aftale standardkontraktbestemmelser eller bindende virksomhedsregler. Kun hvis dette er upraktisk og/eller umuligt, skal den dataansvarlige, ifølge Artikel 29-gruppen, overveje at anvende undtagelserne i artikel 26, stk. 1.

[727] Safe Harbor-principperne er siden Artikel 29-gruppens udtalelse fra 2005 blevet erstattet af EU-U.S. Privacy Shield. Se mere herom i afsnit 6.2. om overførsel baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, artikel 45.

Artikel 29-gruppen udtaler, at de efter samme logik ønsker at anbefale, at undtagelserne i direktivets artikel 26, stk. 1, fortrinsvist anvendes i situationer, hvor det er upassende eller endog umuligt at foretage overførslen på grundlag af artikel 26, stk. 2.

Artikel 29-gruppen finder det endvidere beklageligt, hvis en multinational virksomhed eller offentlig myndighed planlægger at foretage betydelige dataoverførsler til et tredjeland, uden først at sikre en passende databeskyttelse for overførslen, når de praktiske midler til at opnå en sådan beskyttelse findes (f.eks. kontrakt, bindende virksomhedsregler, konvention).

Dette er især grunden til, at Artikel 29-gruppen anbefaler, at overførsler af personoplysninger, der kan kvalificeres som repeterede overførsler, masseoverførsler eller strukturelle overførsler, i givet fald og netop på grund af disse vigtige karakteristika gennemføres inden for rammerne af specifikke retlige rammer (dvs. kontrakter eller bindende virksomhedsregler). Artikel 29-gruppen udtaler imidlertid, at de erkender, at der kan opstå situationer, hvor masseoverførsler eller repeterede overførsler på retmæssig vis kan foretages på grundlag af artikel 26, stk. 1, hvis det i praksis ikke er muligt at anvende dette retlige grundlag, og når den registrerede kun er udsat for en begrænset risiko og artikel 6, 7 og 8 anvendes korrekt. Det kan, ifølge Artikel 29-gruppen, f.eks. dreje sig om internationale pengeoverførsler, der finder sted dagligt og i stort omfang.

Artikel 29-gruppen udtaler endvidere, at selv i de situationer, hvor overførslen betragtes som lovlig i medfør af artikel 26, stk. 1, anbefaler de, at den dataansvarlige på grundlag af en række supplerende faktorer, herunder omfanget af den planlagte overførsel eller risiciene for de registrerede, indgår en kontrakt eller udarbejder bindende virksomhedsregler med henblik på overførsel.

Endelig bør anvendelsen af undtagelserne i artikel 26, stk. 1, ifølge Artikel 29-gruppen, aldrig føre til en krænkelse af de grundlæggende rettigheder.

Artikel 29-gruppen udtaler desuden, at da den europæiske lovgiver indførte disse undtagelser til princippet om tilstrækkelig beskyttelse i direktivet, anså han disse undtagelser for at være begrundede, fordi de blev betragtet som forenelige med beskyttelsen af fysiske personers grundlæggende rettigheder og den fri bevægelighed for information. Mens der i de situationer, der er nævnt i artikel 26, stk. 1, ifølge Artikel 29-gruppen, kan undtages fra princippet om, at tredjelandet skal sikre en tilstrækkelig beskyttelse, danner de med andre ord ikke grundlag for yderligere undtagelser fra de grundlæggende rettigheder.

Ifølge Artikel 29-gruppen skal de nationale databeskyttelsesmyndigheder sørge for, at disse undtagelser anvendes således, at der ikke sker en krænkelse af de registreredes grundlæggende rettigheder, og på en måde, som er i overensstemmelse med en restriktiv fortolkning af disse undtagelser. Myndighederne har, ifølge Artikel 29-gruppen, såfremt der er tilstrækkelig grundlag herfor, i denne henseende mulighed for at gribe ind på ethvert tidspunkt og anbefale, at en international dataoverførsel foretages med tilstrækkelige garantier i den i artikel 26, stk. 2, anvendte betydning i stedet for på grundlag af undtagelserne i artikel 26, stk. 1.

Sammenfattende kan det udledes af Artikel 29-gruppens udtalelse, at direktivets artikel 26, stk. 1 (og dermed også persondatalovens § 27, stk. 3), 1) skal fortolkes restriktivt, 2) at bestemmelserne ikke bør benyttes i forhold til overførsler, der kan kvalificeres som repeterede overførsler, masseoverførsler eller strukturelle overførsler, og 3) at bestemmelserne fortrinsvis bør benyttes som overførselsgrundlag i situationer, hvor det er upassende eller endog umuligt at foretage overførslen på grundlag af artikel 26, stk. 2 (persondatalovens § 27, stk. 4), herunder f.eks. ved brug af Kommissionens standardkontraktbestemmelser eller bindende virksomhedsregler.

Med ovenstående generelle betragtninger in mente vil der i det følgende blive foretaget en gennemgang af de enkelte bestemmelser i persondatalovens § 27, stk. 3.

6.6.2.2. Gennemgang af de enkelte bestemmelser i persondatalovens § 27, stk. 3, nr. 1-8

6.6.2.2.1. Persondatalovens § 27, stk. 3, nr. 1 – samtykke

Af persondataloven § 27, stk. 3, nr. 1, fremgår det, at der kan overføres personoplysninger til et tredjeland, hvis den registrerede har givet sit udtrykkelige samtykke dertil.

Bestemmelsen svarer stort set til artikel 26, stk. 1, litra a, i databeskyttelsesdirektivet, hvoraf det fremgår, at der kan ske overførsel, hvis der ikke hersker tvivl om, at den registrerede har givet sit samtykke.

Det fremgår af bemærkningerne til persondataloven, at samtykkekravet i § 27, stk. 1, nr. 1, skal forstås i overensstemmelse med den legale definition i persondatalovens § 3, nr. 8.[728] Dette indebærer, at samtykket, for at være gyldigt, skal være frivilligt, specifikt og informeret.

[728] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 27, stk. 1, nr. 1.

I forhold til hvilke oplysninger den registrerede som minimum skal oplyses ved overførsel til et tredjeland baseret på et samtykke, fremgår det af bemærkningerne, at den registrerede skal oplyses om, hvilke typer af oplysninger der overføres, til hvilke formål og til hvilke tredjelande. Herudover vil der skulle gives andre relevante oplysninger, som kan have betydning for den registreredes vurdering af risikoen ved overførslen.

Artikel 29-gruppen har, i forhold til kravet om at et samtykke skal være *specifikt*, i WP 114 bl.a. udtalt, at kravet indebærer, at det i visse situationer vil være umuligt at opnå den registreredes forudgående samtykke for en fremtidig overførsel. Dette vil f.eks. være tilfældet, hvis man på det tidspunkt, hvor der anmodes om samtykke, ikke har kendskab til en eventuel fremtidig overførsel eller de omstændigheder, under hvilke en sådan overførsel vil finde sted, således at det ikke er muligt at vurdere konsekvenserne af denne overførsel for den registrerede.

For så vidt angår kravet om, at et samtykke skal være *informeret*, har Artikel 29-gruppen i WP 114 bl.a. udtalt, at kravet indebærer, at den information, som de registrerede modtager, også skal beskrive de specifikke risici, der er forbundet med overførslen af deres oplysninger til et tredjeland, der ikke sikrer en tilstrækkelig beskyttelse.

6.6.2.2.2. Persondatalovens § 27, stk. 3, nr. 2 – aftale mellem den registrerede og den dataansvarlige

Det fremgår af persondatalovens § 27, stk. 3, nr. 2, at der kan ske overførsel af personoplysninger til et tredjeland, hvis overførslen er nødvendig af hensyn til opfyldelsen af en aftale mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan aftale.

Bestemmelsen svarer til artikel 26, stk. 1, litra b, i databeskyttelsesdirektivet.

Artikel 29-gruppen har i WP 114 udtalt, at en restriktiv fortolkning af artikel 26, stk. 1, litra b, må betyde, at de oplysninger, der overføres, virkelig skal være nødvendige for opfyldelsen af en aftale mellem den registrerede og den dataansvarlige eller gennemførelsen af foranstaltninger, der træffes forud for indgåelsen af aftalen.

På denne baggrund finder Artikel 29-gruppen f.eks., at det er tvivlsomt, om bestemmelsen kan benyttes af internationale koncerner med henblik på at overføre oplysninger om deres ansatte fra et datterselskab til moderselskabet, bl.a. for at centralisere koncernens betalinger og HR.

Artikel 29-gruppen har endvidere i sin udtalelse af 24. oktober 2002 om overførsel af passagerlisteoplysninger (såkaldte PNR-oplysninger[729]) og andre oplysninger fra luftfartsselskaber til USA (WP 66) udtalt, at artikel 26, stk. 1, litra b, ikke kan finde anvendelse på overførsel af oplysninger om flypassagerer til amerikanske myndigheder, idet overførslerne ikke kan siges at være nødvendige for opfyldelsen af aftalen mellem en flypassager og et luftfartsselskab.

Det skal i den forbindelse bemærkes, at Datatilsynet i sin praksis har anlagt et andet synspunkt end Artikel 29-gruppen for så vidt angår PNR-oplysninger.[730] Datatilsynet har således i sin praksis accepteret, at persondatalovens § 27, stk. 3, nr. 2, efter omstændighederne, kan anvendes som hjemmel i forbindelse med luftfartsselskabers overførsel af oplysninger om deres passagerer til de amerikanske toldmyndigheder med henblik på at opfyldes deres aftaler med de enkelte passagerer.

I forhold til, hvornår artikel 26, stk. 1, litra b, kan anvendes, har Artikel 29-gruppen i WP 114 udtalt, at dette kan ske ved rejsebureauers overførsel af personoplysninger vedrørende deres kunder til hoteller eller andre forretningspartnere, der deltager i organisationen af kundernes rejser.

Af særlig betydning i dansk kontekst skal det bemærkes, at kravet om at den registrerede er part i den pågældende aftale, som skal opfyldes, eller er på vej til at blive aftalepart, må antages at indebære, at alene individuelle aftaler kan danne grundlag for overførsler efter artikel 26, stk. 1, litra b. Dette kan således ikke antages at kunne ske på grundlag af kollektive aftaler, såsom overenskomster mv.[731]

6.6.2.2.3. Persondatalovens § 27, stk. 3, nr. 3 – aftale i den registreredes interesse, der er indgået mellem den dataansvarlige og tredjemand

Af persondatalovens § 27, stk. 3, nr. 3, fremgår det, at der kan ske overførsel af personoplysninger til et tredjeland, hvis overførslen er nødvendig af hensyn til indgåelsen eller udførelsen af en aftale, der i den registreredes interesse er indgået mellem den dataansvarlige og tredjemand.

Bestemmelsen svarer til artikel 26, stk. 1, litra c, i databeskyttelsesdirektivet.

[729] PNR står for Passenger Name Record.
[730] Reservationssystem (RESAID), Datatilsynets j.nr. 2003-42-0516.
[731] Persondataloven med kommentarer (2015), s. 452.

Det fremgår af bemærkningerne til persondataloven[732], at bestemmelsen f.eks. kan anvendes ved overførsel af personoplysninger med henblik på at gennemføre betalingsoverførsler til eller fra et tredjeland, som enten aftales mellem den registrerede og den dataansvarlige, eller som blot er i den registreredes interesse.

Umiddelbart synes bemærkningerne til persondatalovens § 27, stk. 3, nr. 3, både at omhandle situationer, der er omfattet af lovens § 27, stk. 3, nr. 2 og 3.

Artikel 29-gruppen har i WP 114 givet nogle eksempler på situationer, hvor bestemmelsen i databeskyttelsesdirektivets artikel 26, stk. 1, litra c – efter gruppens opfattelse – *ikke* finder anvendelse. Artikel 29-gruppen har f.eks. udtalt, at visse dataansvarlige har udtrykt ønske om at anvende artikel 26, stk. 1, litra c, som grundlag for internationale overførsler af oplysninger vedrørende deres ansatte til tjenesteydere, der er etableret uden for EU, og hvortil de har overdraget lønudbetalingen. Disse dataansvarlige har overfor Artikel 29-gruppen anført, at overførslerne er nødvendige for opfyldelsen af deres kontrakt om underleverance, og at overførslen i øvrigt er i de registreredes interesse, eftersom formålet med overførslen er udbetaling af løn til de ansatte. I disse tilfælde er Artikel 29-gruppen imidlertid af den opfattelse, at man ikke kan påvise nogen tæt og betydelig forbindelse mellem den registreredes interesser og kontraktens formål, hvorfor undtagelsen ikke kan finde anvendelse.

6.6.2.2.4. Persondatalovens § 27, stk. 3, nr. 4 – nødvendig eller følger af lov for at beskytte en vigtig samfundsmæssig interesse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares

Det fremgår af persondatalovens § 27, stk. 3, nr. 4, at der kan ske overførsel af personoplysninger til et tredjeland, hvis overførslen er nødvendig eller følger af lov eller bestemmelser fastsat i henhold til lov for at beskytte en vigtig samfundsmæssig interesse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

Bestemmelsen, der svarer til artikel 26, stk. 1, litra d, i databeskyttelsesdirektivet, giver mulighed for, at der kan ske overførsel til tredjelande i to situationer.

For det første kan der ske overførsel, hvis det er nødvendigt eller følger af lov eller bestemmelser fastsat i henhold til lov for at beskytte en *vigtig samfundsmæssig interesse*.

[732] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 27, stk. 1, nr. 3.

Som et eksempel på en overførsel, der vil være omfattet af bestemmelsen, peges der i bemærkningerne til persondataloven på den situation, hvor der sker international udveksling af oplysninger mellem skatte- og toldmyndigheder eller mellem socialsikringsmyndigheder.[733]

For det andet kan der ske overførsel, hvis det er nødvendigt for, at *et retskrav kan fastlægges, gøres gældende eller forsvares*.

Af bemærkningerne til persondataloven fremgår det, at udtrykket *retskrav* skal forstås på samme måde som i bestemmelsen i lovens § 7, stk. 2, nr. 4.

6.6.2.2.5. Persondatalovens § 27, stk. 3, nr. 5 – for at beskytte den registreredes vitale interesser

Af persondatalovens § 27, stk. 3, nr. 5, fremgår det, at der kan ske overførsel af personoplysninger til et tredjeland, hvis overførslen er nødvendig for at beskytte den registreredes vitale interesser.

Bestemmelsen svarer til artikel 26, stk. 1, litra e, i databeskyttelsesdirektivet.

Det fremgår af bemærkningerne til persondataloven, at bestemmelsen svarer til lovens § 6, stk. 1, nr. 4.

Artikel 29-gruppen har i WP 114 udtalt, at artikel 26, stk. 1, litra e, finder anvendelse ved overførsel af oplysninger i tilfælde af en medicinsk nødsituation, hvor oplysningerne betragtes som nødvendige for at give den påkrævede lægehjælp.

Ifølge Artikel 29-gruppen skal det således være muligt på retmæssig vis at overføre oplysninger (herunder visse personoplysninger), hvis den registrerede er bevidstløs og har brug for øjeblikkelig lægehjælp, og hvis det kun er den registreredes egen læge, der er etableret i en EU-medlemsstat, der er i stand til at give disse oplysninger.

Artikel 29-gruppen understreger dog også, at overførslen skal vedrøre den registreredes individuelle interesser, og den skal med hensyn til helbredsoplysninger være nødvendig for at kunne stille en diagnose. Artikel 26, stk. 1, litra e, kan derfor ikke anvendes som begrundelse for at overføre medicinske personoplysninger til personer, der er ansvarlige for behandlingen, og som er etableret uden for EU, hvis de ikke har til opgave at behandle den

[733] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 27, stk. 1, nr. 4.

registrerede i en konkret situation, men f.eks. agter at foretage generel medicinsk forskning, hvoraf resultaterne først vil foreligge på længere sigt.

6.6.2.2.6. Persondatalovens § 27, stk. 3, nr. 6 – overførsel finder sted fra et register, der ifølge lov er tilgængeligt for offentligheden m.fl., idet omfang de i lovgivningen fastsatte betingelser for offentlig tilgængelighed er opfyldt

Det fremgår af persondatalovens § 27, stk. 3, nr. 6, at der kan ske overførsel af personoplysninger til et tredjeland, hvis overførslen finder sted fra et register, der ifølge lov eller bestemmelser fastsat i henhold til lov er tilgængeligt for offentligheden eller for personer, der kan godtgøre at have en berettiget interesse heri, i det omfang de i lovgivningen fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde.

Bestemmelsen svarer stort set til artikel 26, stk. 1, litra f, i databeskyttelsesdirektivet.

Af bemærkningerne til persondataloven – der henviser til databeskyttelsesdirektivets præambelbetragtning nr. 58 – fremgår det, at § 27, stk. 3, nr. 6, kun finder anvendelse, hvis de i lovgivningen fastsatte betingelser for den offentlige tilgængelighed er opfyldt i det specifikke tilfælde.[734] Det fremgår endvidere, at adgangen til efter bestemmelsen at overføre oplysninger ikke omfatter alle oplysninger eller hele kategorier af oplysninger i registeret.

Artikel 29-gruppen har i WP 114, om begrænsningen i forhold til, at ikke alle oplysninger eller hele kategorier af oplysninger kan overføres, udtalt, at det ikke vil være i overensstemmelse med ånden i artikel 26, stk. 1, litra f, hvis dette retlige grundlag for overførsel bliver anvendt til at tømme disse registre for deres indhold med risiko for, at tredjelandes anvendelse af disse kan føre til en anden anvendelse end den, de oprindelig var udarbejdet til.

Som et eksempel på hvornår bestemmelsen kan anvendes, peger Artikel 29-gruppen på, at man kan forestille sig, at bestemmelsen kan blive anvendt – i overensstemmelse med den nationale lovgivning – af en person, der er født i en EU-medlemsstat, men bor i et tredjeland, for at indhente udskrifter fra folkeregistret på sit fødested med henblik på et permanent ophold i sit nye opholdsland.

6.6.2.2.7. Persondatalovens § 27, stk. 3, nr. 7 og 8 – af hensyn til forebyggelse, efterforskning og forfølgelse af strafbare forhold samt af hensyn til den offentlige sikkerhed mv.

Af persondatalovens § 27, stk. 3, nr. 7 og 8, fremgår det, at der kan ske overførsel af personoplysninger til et tredjeland, hvis overførslen er nødvendig af hensyn til forebyggelse,

[734] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 27, stk. 1, nr. 6.

efterforskning og forfølgning af strafbare forhold samt straffuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig forfølgning (nr. 7), eller overførslen er nødvendig af hensyn til den offentlige sikkerhed, rigets forsvar eller statens sikkerhed (nr. 8).

Det fremgår af bemærkningerne til persondataloven, bestemmelserne er indsat for at tydeliggøre, at den nødvendige behandling i de nævnte øjemed kan finde sted.[735] Endvidere bemærkes det, at en sådan behandling falder uden for direktivets område, jf. artikel 3, stk. 2, 1. pind, 2. led, og at bestemmelserne således er indsat uafhængigt af direktivets regulering.

Fra Datatilsynets praksis vedrørende bestemmelsen kan der peges på tilsynet sag med j.nr. 2005-321-0417. Sagen angik spørgsmålet om dansk politis udveksling af visse pasoplysninger med den internationale politiorganisation Interpol på baggrund af en fælles holdning af 24. januar 2006 vedtaget i EU. Efter den fælles holdning (som ikke kan anses for retligt bindende) skal medlemsstaterne udveksle oplysninger om pasnummer, udstedelsesland og dokumenttype vedrørende stjålne, bortkomne eller ulovligt handlede udstedte pas eller blankopas med Interpol. Formålet hermed er at forhindre og bekæmpe alvorlig og organiseret kriminalitet, herunder terrorisme. Datatilsynet udtalte bl.a., at tilsynet ikke fandt grundlag for at tilsidesætte Justitsministeriets og Rigspolitiets vurdering af, at overførslen af pasoplysninger kunne ske med hjemmel i persondatalovens § 27, stk. 3, nr. 7 og 8.

6.6.3. Databeskyttelsesforordningen

6.6.3.1. Databeskyttelsesforordningens artikel 49, stk. 1 – overførsel af personoplysninger til tredjelande i situationer, hvor tredjelandet ikke har et tilstrækkeligt beskyttelsesniveau, og hvor der heller ikke er givet fornødne garantier

6.6.3.1.1. Databeskyttelsesforordningens artikel 49, stk. 1, første afsnit

Det fremgår af databeskyttelsesforordningens artikel 49, stk. 1, første afsnit, at der i mangel af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 45, stk. 3, eller fornødne garantier i henhold til artikel 46, herunder bindende virksomhedsregler, kun må ske overførsel af personoplysninger til et tredjeland eller en international organisation, hvis en af følgende betingelser er opfyldt:

> a) den registrerede udtrykkelig har givet samtykke til den foreslåede overførsel efter at være blevet informeret om de mulige risici, som sådanne overførsler kan medføre for den registrerede på grund af den manglende

[735] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 27, stk. 1, nr. 7 og 8.

afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller fornødne garantier

b) overførslen er nødvendig af hensyn til opfyldelse af en kontrakt mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en sådan kontrakt

c) overførslen er nødvendig af hensyn til indgåelse eller opfyldelse af en kontrakt, der i den registreredes interesse indgås mellem den dataansvarlige og en anden fysisk eller juridisk person

d) overførslen er nødvendig af hensyn til vigtige samfundsinteresser

e) overførslen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares

f) overførslen er nødvendig for at beskytte den registreredes eller andre personers vitale interesser, hvis den registrerede ikke fysisk eller juridisk er i stand til at give samtykke

g) overførslen finder sted fra et register, der ifølge EU-ret eller medlemsstaternes nationale ret er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri, men kun i det omfang de ved EU-ret eller medlemsstaternes nationale ret fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde.

Af præambelbetragtning nr. 111 fremgår det om undtagelserne i artikel 49, stk. 1, første afsnit, at en overførsel bør tillades under visse omstændigheder, når den registrerede har givet sit udtrykkelige samtykke, og hvor overførslen er lejlighedsvis og nødvendig i forbindelse med en kontrakt eller et retskrav, uanset om det sker i forbindelse med en retssag eller en administrativ eller udenretslig procedure, herunder procedurer ved reguleringsorganer. Endvidere fremgår det, at en overførsel også bør tillades, når vigtige samfundsinteresser i henhold til EU-retten eller medlemsstaternes nationale ret kræver det, eller når en overførsel sker fra et register, der er oprettet ved lov, og som er tilgængeligt for offentligheden eller personer med en legitim interesse. Om sidstnævnte tilfælde fremgår det tillige, at en sådan overførsel ikke bør omfatte alle personoplysningerne eller alle kategorier af oplysninger i registeret, og når registeret er beregnet til at blive konsulteret af personer, der

har en legitim interesse, bør overførsel under fuld hensyntagen til den registreredes interesser og grundlæggende rettigheder kun ske på anmodning af disse personer, eller hvis de skal være modtagere.

Herudover fremgår det af præambelbetragtning 112, at undtagelserne i artikel 49 navnlig bør gælde for overførsel af oplysninger, der foretages af hensyn til vigtige samfundsinteresser, f.eks. international udveksling af oplysninger mellem konkurrencemyndigheder, skatte- eller toldforvaltninger, finansielle tilsynsmyndigheder eller socialsikringsmyndigheder eller med henblik på folkesundhed, f.eks. i tilfælde af kontaktopsporing i forbindelse med smitsomme sygdomme eller for at nedbringe og/eller afskaffe doping inden for sport. Endvidere fremgår det, at en overførsel af personoplysninger, der er nødvendig for at beskytte et hensyn af fundamental betydning for den registreredes eller en anden persons vitale interesser, herunder fysisk integritet eller liv, ligeledes bør anses for lovlig, hvis den registrerede er ude af stand til at give sit samtykke. Det fremgår tillige, at enhver overførsel til en international humanitær organisation af personoplysninger om en registreret, der ikke fysisk eller juridisk er i stand til at give sit samtykke, med henblik på udførelse af en opgave i henhold til Genèvekonventionerne eller for at overholde international humanitær ret, som finder anvendelse i væbnede konflikter, kan anses for at være nødvendig af hensyn til vigtige samfundsinteresser, eller fordi det er af vital interesse for den registrerede.

Når bestemmelserne i databeskyttelsesforordningens artikel 49, stk. 1, første afsnit, sammenholdes med gældende ret, kan det konstateres, at artikel 49, stk. 1, første afsnit, litra b, c, d, e og g – til trods for enkelte sproglige omformuleringer – er videreførelser af gældende ret. Dog er det nyt, at bestemmelserne i litra d og e nu optræder i separate bestemmelser.

For så vidt angår artikel 49, stk. 1, første afsnit, litra a, om samtykke, er samtykkekravet ændret fra, at der, efter direktivet, ikke må herske tvivl om, at den registrerede har givet sit samtykke til, at den registrerede, efter forordningen, skal have givet sit udtrykkelige samtykke. På denne måde ligner forordningens krav det krav om udtrykkeligt samtykke, der i dag fremgår af persondatalovens § 27, stk. 3, nr. 1. I praksis vil det næppe gøre en forskel, at ordlyden af samtykkekravet ændres, hvorfor forordningens artikel 49, stk. 1, første afsnit, litra a, vil være en videreførelse af gældende ret. At det fremgår direkte af artikel 49, stk. 1, første afsnit, litra a, at den registrerede skal være blevet informeret om de mulige risici, som overførslerne kan medføre for den registrerede, er nyt. Tilføjelsen indebærer dog ikke en ændring af gældende ret, idet Artikel 29-gruppen i WP 114 har fastslået, at kravet om at et samtykke skal være informeret bl.a. indebærer, at den registrerede skal oplyses om de risici, der er forbundet med overførslen.

I forhold til artikel 49, stk. 1, første afsnit, litra f, er det nyt, at en overførsel også kan ske, når det er nødvendigt for at beskytte andre personers vitale interesser. Efter databeskyttelsesdirektivets artikel 26, stk. 1, litra e, kan der kun ske overførsel, når det er nødvendigt for at beskytte den registreredes vitale interesser. Det må umiddelbart antages, at udvidelsen i artikel 49, stk. 1, første afsnit, litra f, vil dække relativt få situationer, da udvidelsen må skulle fortolkes i lyset af Artikel 29-gruppens udtalelse i WP 114, jf. ovenfor. Overførsler vil således kun kunne ske, hvis der f.eks. er tale om en medicinsk nødsituation, hvor oplysningerne er nødvendige for at give en anden person den påkrævede lægehjælp, og hvor den registrerede ikke fysisk eller juridisk er i stand til at give samtykke.

6.6.3.1.2. Databeskyttelsesforordningens artikel 49, stk. 1, andet afsnit

Endvidere fremgår det af stk. 1, andet afsnit, at hvis en overførsel ikke kan have hjemmel i en bestemmelse i artikel 45 eller 46, herunder bestemmelserne om bindende virksomhedsregler, og ingen af undtagelserne i særlige situationer omhandlet i dette stykkes første afsnit finder anvendelse, må en *videregivelse* til et tredjeland eller en international organisation kun finde sted, hvis 1) overførslen ikke gentages, 2) kun vedrører et begrænset antal registrerede, 3) er nødvendig af hensyn til vægtige legitime interesser, som forfølges af den dataansvarlige, 4) den registreredes interesser eller rettigheder og frihedsrettigheder ikke går forud for disse interesser, og 5) den dataansvarlige har vurderet alle omstændigheder i forbindelse med overførslen og på grundlag af denne vurdering giver passende garantier for beskyttelse af personoplysningerne. Endvidere fremgår det, at den dataansvarlige skal underrette tilsynsmyndigheden om overførslen. Ud over oplysningerne i artikel 13 og 14 underretter den dataansvarlige den registrerede om overførslen og om de vægtige legitime interesser, der forfølges.

Om artikel 49, stk. 1, andet afsnit, fremgår det af præambelbetragtning nr. 113, at overførsler, der ikke kan betegnes som værende præget af gentagelser, og som kun vedrører et begrænset antal registrerede, også kan være mulig af hensyn til vægtige legitime interesser, som forfølges af den dataansvarlige, hvis den registreredes interesser eller rettigheder og frihedsrettigheder ikke går forud for disse interesser, og hvis den dataansvarlige har vurderet alle omstændigheder i forbindelse med overførslen. I forhold til hvad der skal lægges vægt på ved denne vurdering fremgår det, at den dataansvarlige bør lægge særlig vægt på de pågældende personoplysningers karakter, formålet med og varigheden af den eller de foreslåede behandlinger samt situationen i oprindelseslandet, tredjelandet og det endelige bestemmelsesland og bør give fornødne garantier for beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder med hensyn til behandling af deres personoplysninger. Det fremgår endvidere, at en sådan overførsel kun bør være mulig i enkelttilfælde, hvor ingen af de andre grunde til overførsel kan finde anvendelse. Herudover fremgår det, at med henblik på videnskabelige eller historiske forskningsformål eller stati-

stiske formål bør samfundets legitime forventninger om øget viden tages med i overvejelserne. Den dataansvarlige bør underrette tilsynsmyndigheden og den registrerede om overførslen.

Indledningsvist skal det bemærkes, at der må være tale om en oversættelsesfejl, når der i tredje linje i artikel 49, stk. 1, andet afsnit, benyttes ordet "videregivelse". I den engelske version af databeskyttelsesforordningen står der således også "transfer", hvilket burde have været oversat til "overførsel".

For så vidt angår selve indholdet af artikel 49, stk. 1, andet afsnit, introduceres der med bestemmelsen en helt ny hjemmel til overførsel til tredjelande. Bestemmelsen er en interesseafvejningsregel, og den har karakter af en slags opsamlingsbestemmelse i forhold til de øvrige bestemmelser i artikel 49, stk. 1.

Bestemmelsen i artikel 49, stk. 1, andet afsnit, vil næppe blive anvendt ret ofte i praksis, da der opstilles strenge krav for bestemmelsens anvendelse, herunder at ingen af de andre grunde til overførsel kan finde anvendelse. Den dataansvarlige vil tillige skulle underrette både tilsynsmyndigheden og den registrerede om overførslen.

6.6.3.2. Databeskyttelsesforordningens artikel 49, stk. 2 – særlig begrænsning i forhold til stk. 1, første afsnit, litra g)

Af databeskyttelsesforordningens artikel 49, stk. 2, fremgår det, at en overførsel i henhold til stk. 1, første afsnit, litra g, ikke må omfatte alle personoplysninger eller hele kategorier af personoplysninger i et register. Det fremgår tillige, at når et register er beregnet til at blive konsulteret af personer, der har en legitim interesse heri, må overførsel kun ske på anmodning af disse personer, eller hvis de skal være modtagerne.

Bestemmelsen i artikel 49, stk. 2, er en gengivelse af dele af databeskyttelsesdirektivets præambelbetragtning 58. Der er således tale om en videreførelse af gældende ret.

6.6.3.3. Databeskyttelsesforordningens artikel 49, stk. 3 – særlige begrænsninger i forhold til stk. 1, første afsnit litra a, b og c og stk. 1, andet afsnit

Det fremgår af databeskyttelsesforordningens artikel 49, stk. 3, at stk. 1, første afsnit, litra a, b og c, og stk. 1, andet afsnit, ikke finder anvendelse på aktiviteter, der gennemføres af offentlige myndigheder som led i udøvelsen af deres offentligretlige beføjelser.

Som noget nyt begrænser forordningens artikel 49, stk. 3, offentlige myndigheders mulighed for at benytte bestemmelserne i artikel 49, stk. 1, første afsnit, litra a, b og c, som hjemmel ved overførsel af personoplysninger til tredjelande. Den praktiske betydning af

artikel 49, stk. 3, er næppe ret stor, da det må antages, at offentlige myndigheder – måske med undtagelse af enkelte myndigheder, der beskæftiger sig med forskning – i forvejen meget sjældent benytter de pågældende bestemmelser som overførselsgrundlag.

Herudover medfører artikel 49, stk. 3, at offentlige myndigheder *ved aktiviteter, der gennemføres som led i udøvelse af deres offentligretlige beføjelser*, heller ikke kan benytte den nye interesseafvejningsregel i artikel 49, stk. 1, andet afsnit. Dette er fint i tråd med, at offentlige myndigheder *ved behandling, som foretages som led i udførelsen af deres opgaver*, som noget nyt med forordningen, heller ikke vil kunne benytte interesseafvejningsreglen i forordningens artikel 6, stk. 1, litra f.

6.6.3.4. Databeskyttelsesforordningens artikel 49, stk. 4 – særlig begrænsning i forhold til stk. 1, første afsnit, litra d

Af databeskyttelsesforordningens artikel 49, stk. 4, fremgår det, at de samfundsinteresser, der er omhandlet i stk. 1, første afsnit, litra d, skal være anerkendt i EU-retten eller retten i den medlemsstat, som den dataansvarlige er underlagt.

Bestemmelsen i forordningens artikel 49, stk. 4, er umiddelbart en videreførelse af gældende ret.

6.6.3.5. Databeskyttelsesforordningens artikel 49, stk. 5 – EU-retten eller medlemsstaternes nationale ret kan udtrykkeligt fastsætte grænser for overførsel af særlige kategorier af oplysninger

Det fremgår af databeskyttelsesforordningens artikel 49, stk. 5, at hvis der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, kan EU-retten eller medlemsstaternes nationale ret, af hensyn til vigtige samfundsinteresser, udtrykkeligt fastsætte grænser for overførsel af særlige kategorier af oplysninger til et tredjeland eller en international organisation. Endvidere fremgår det, at medlemsstaterne skal give EU-Kommissionen meddelelse om sådanne bestemmelser.

Artikel 49, stk. 5, giver mulighed for, at man i Danmark kan fastsætte grænser for overførsel af særlige kategorier af oplysninger til et tredjeland eller en international organisation, når der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

Det skal i øvrigt bemærkes, at muligheden for at medlemsstaterne kan fastsætte regler om, at bestemmelserne ikke skal gælde i bestemte tilfælde, ikke er ny, idet denne mulighed også fremgår af databeskyttelsesdirektivets artikel 26, stk. 1, der er gennemført i dansk ret ved persondatalovens § 27, stk. 3.

6.6.3.6. Databeskyttelsesforordningens artikel 49, stk. 6 – dokumentation af vurdering efter stk. 1, andet afsnit

Af databeskyttelsesforordningens artikel 49, stk. 6, fremgår det, at den dataansvarlige eller databehandleren skal dokumentere vurderingen og de passende garantier i denne artikels stk. 1, andet afsnit, i de fortegnelser, der er omhandlet i artikel 30.

Bestemmelsen er ny, og den er umiddelbart en konsekvens af bestemmelserne i forordningens artikel 30, stk. 1, litra e (dataansvarlige), og artikel 30, stk. 2, litra c (databehandlere). Se mere herom i afsnit 5.7. om fortegnelser over behandlingsaktiviteter, artikel 30, stk. 1-4.

6.6.4. Overvejelser

For så vidt angår databeskyttelsesforordningens artikel 49, stk. 1, første afsnit, er litra b, c, d, e og g – til trods for enkelte sproglige omformuleringer – videreførelser af gældende ret. Dog er det nyt, at bestemmelserne i litra d og e nu optræder i separate bestemmelser.

Forordningens artikel 49, stk. 1, første afsnit, litra a, må i praksis også antages at være en videreførelse af gældende ret, selvom samtykkekravet er blevet ændret fra, at der, efter direktivet, ikke må herske tvivl om, at den registrerede har givet sit samtykke til, at den registrerede, efter forordningen, skal have givet sit udtrykkelige samtykke. At det, som noget nyt, fremgår af artikel 49, stk. 1, første afsnit, litra a, at den registrerede skal være blevet informeret om de mulige risici, som overførslerne kan medføre for den registrerede, indebærer ikke en ændring af gældende ret, i det et sådan krav allerede følger af Artikel 29-gruppens udtalelser.

I forhold til artikel 49, stk. 1, første afsnit, litra f, da er det nyt, at en overførsel også kan ske, når det er nødvendigt for at beskytte andre personers vitale interesser. Det må umiddelbart antages, at udvidelsen i artikel 49, stk. 1, første afsnit, litra f, vil dække relativt få situationer, da udvidelsen må skulle fortolkes i lyset af Artikel 29-gruppens udtalelse i WP 114, jf. ovenfor.

For så vidt angår selve indholdet af artikel 49, stk. 1, andet afsnit, da introduceres der med bestemmelsen en helt ny hjemmel til overførsel til tredjelande. Bestemmelsen i artikel 49, stk. 1, andet afsnit, vil næppe blive anvendt ret ofte i praksis, da der opstilles strenge krav for bestemmelsens anvendelse, herunder at ingen af de andre grunde til overførsel kan finde anvendelse.

Bestemmelsen i forordningens artikel 49, stk. 2, er en gengivelse af dele af databeskyttelsesdirektivets præambelbetragtning nr. 58. Der er således tale om en videreførelse af gældende ret.

Forordningens artikel 49, stk. 3, begrænser, som noget nyt, offentlige myndigheders mulighed for at benytte bestemmelserne i artikel 49, stk. 1, første afsnit, litra a, b og c, som hjemmel ved overførsel af personoplysninger til tredjelande, når myndighederne gennemfører aktiviteter, som led i udøvelsen af deres offentligretlige beføjelser. Den praktiske betydning af artikel 49, stk. 3, er næppe ret stor, da det må antages, at offentlige myndigheder – måske med undtagelse af enkelte myndigheder, der beskæftiger sig med forskning – i forvejen meget sjældent benytter de pågældende bestemmelser som overførselsgrundlag.

Bestemmelsen i forordningens artikel 49, stk. 4, er umiddelbart en videreførelse af gældende ret.

Forordningens artikel 49, stk. 5, giver mulighed for, at man i Danmark kan fastsætte grænser for overførsel af særlige kategorier af oplysninger til et tredjeland eller en international organisation, når der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

Bestemmelsen i artikel 49, stk. 6, er ny, og den er umiddelbart en konsekvens af bestemmelserne i forordningens artikel 30, stk. 1, litra e (dataansvarlige), og artikel 30, stk. 2, litra c (databehandlere).

6.7. Internationalt samarbejde om beskyttelse af personoplysninger, artikel 50

6.7.1. Præsentation

Databeskyttelsesforordningens artikel 50 fastsætter regler om, at Kommissionen og de nationale tilsynsmyndigheder – i forhold til tredjelande og internationale organisationer – skal træffe de nødvendige foranstaltninger til at udvikle internationale samarbejdsmekanismer og yde gensidig bistand mv.

Bestemmelsen, der er indsat som sidste bestemmelse i databeskyttelsesforordningens kapitel V om overførsel af personoplysninger til tredjelande og internationale organisationer, er ny i forhold til persondataloven og databeskyttelsesdirektivet, idet disse ikke indeholder lignende udtrykkelige regler.

I praksis er det derimod ikke nyt, at både EU-Kommissionen og de nationale tilsynsmyndigheder i et vist omfang deltager i internationalt samarbejde om beskyttelse af personoplysninger.

6.7.2. Gældende ret

Som nævnt indeholder hverken databeskyttelsesdirektivet eller persondataloven udtrykkelige regler om en forpligtelse til at samarbejde internationalt. Der har imidlertid med årene udviklet sig en række af sådanne samarbejder, som nationale tilsynsmyndigheder allerede i dag er involveret i.

6.7.2.1. Global Cross Border Enforcement Cooperation Arrangement

Global Cross Border Enforcement Cooperation Arrangement er et grænseoverskridende håndhævelsessamarbejde mellem tilsynsmyndigheder fra hele verden, herunder fra EU.

Samarbejdet udspringer af en resolution fra den 36. internationale databeskyttelseskonference, som afholdes hvert år.

Formålet med samarbejdet er ifølge samarbejdsdokumentet bl.a. at fremme efterlevelse af databeskyttelsesregler hos organisationer, der behandler personoplysninger på tværs af landegrænser.

Midlerne til at opnå formålet er ifølge samarbejdsdokumentet (I) at udstikke retningslinjer for udveksling af håndhævelsesrelaterede oplysninger samt at udstikke retningslinjer for, hvordan sådanne oplysninger skal behandles af modtagerne; (II) at fremme en fælles forståelse for og tilgang til internationalt håndhævelsessamarbejde; (III) at tilskynde deltagerne til at engagere sig i grænseoverskridende tilsynssamarbejde ved at dele håndhævelsesrelateret materiale og – hvor det er passende – at assistere andre deltagere med viden, ekspertise og erfaring og; (IV) at tilskynde deltagerne til at benytte og deltage i udviklingen af sikre elektroniske vidensdelingsplatforme, hvor der kan udveksles håndhævelsesrelaterede oplysninger, herunder især fortrolige oplysninger om igangværende eller fremtidige håndhævelsesaktiviteter.

Datatilsynet deltager pt. ikke i samarbejdet.

6.7.2.2. Global Privacy Enforcement Network (GPEN)

I 2007 vedtog OECD's råd[736] en anbefaling vedrørende grænseoverskridende samarbejde i forbindelse med håndhævelse af databeskyttelsesregler.[737]

Af anbefalingen fremgår det bl.a., at OECD's medlemsstater bør fremme etableringen af et netværk af tilsynsmyndigheder og andre interessenter. I netværket bør de praktiske aspek-

[736] Rådet er det styrende organ i OECD og udgøres af repræsentanter for medlemsstaterne og EU-Kommissionen.
[737] OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.

ter vedrørende samarbejde om håndhævelse af databeskyttelsesregler diskuteres, ligesom der i netværket bør udveksles bedste praksisser i forhold til grænseoverskridende udfordringer. Endelig bør der i netværket udvikles fælles prioriteringer for håndhævelse samt udvikles oplysningskampagner.

Som følge af Rådets anbefaling valgte en række lande i 2010 at etablere GPEN-netværket.

Om GPEN's mission fremgår det af netværkets hjemmeside, at man primært forsøger at fremme samarbejdet ved (I) at udveksle oplysninger om relevante emner, trends og erfaringer; (II) at støtte uddannelsesmuligheder (tænkes formentlig på medarbejderpraktikker) og deling af viden om håndhævelse og bedste praksisser; (III) at fremme dialog med organisationer, der har en rolle i forbindelse med håndhævelse af databeskyttelsesregler; (IV) at udvikle, opretholde og støtte processer og mekanismer, der er brugbare med hensyn til bilateralt eller multilateralt samarbejde og; (V) at iværksætte og støtte specifikke aktiviteter relateret til GPEN's mission.

Det fremgår endvidere af GPEN's hjemmeside, at der pt. er 47 medlemmer af GPEN-netværket, og at medlemmerne kommer fra hele verden, men med en overvægt af medlemmer fra Europa. Bl.a. er Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) medlem, ligesom netværket også har et nordisk medlem i form af det norske datatilsyn.

Datatilsynet deltager pt. ikke i GPEN-netværket.

6.7.2.3. Internationalt arbejde i regi af Artikel 29-gruppen

Af databeskyttelsesdirektivets artikel 30, stk. 1, litra b, fremgår det, at Artikel 29-gruppen bl.a. har til opgave, at give EU-Kommissionen udtalelser om beskyttelsesniveauet i Fællesskabet og i *tredjelande*.

I praksis er det typisk i forbindelse med, at EU-Kommissionen, i medfør af databeskyttelsesdirektivets artikel 25, stk. 6, agter at fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, at Artikel 29-gruppen udtaler sig om beskyttelsesniveauet i tredjelande.

Senest har Artikel 29-gruppen deltaget i vurderingen af beskyttelsesniveauet i et tredjeland op til vedtagelsen af det nye EU-U.S. Privacy Shield, hvor EU-Kommissionen ved afgørelse af 12. juli 2016 har fastslået, at amerikanske organisationer, der har tilsluttet sig det nye "shield" sikrer et tilstrækkeligt beskyttelsesniveau i forbindelse med overførsel af personoplysninger fra EU til USA.[738]

[738] Se bl.a. Artikel 29-gruppens udtalelse af 13. april 2016 om EU-U.S. Privacy Shield (WP 238).

6.7.3. Databeskyttelsesforordningen

Det fremgår af databeskyttelsesforordningens artikel 50, at EU-Kommissionen og tilsynsmyndighederne, i forhold til tredjelande og internationale organisationer, træffer de fornødne foranstaltninger til at:

a) Udvikle internationale samarbejdsmekanismer med henblik på at lette effektiv håndhævelse af lovgivningen om beskyttelse af personoplysninger.

b) Yde international gensidig bistand i håndhævelse af lovgivningen om beskyttelse af personoplysninger, herunder gennem anmeldelse, indbringelse af klager, efterforskningsbistand og informationsudveksling, under iagttagelse af de fornødne garantier for beskyttelse af personoplysninger og andre grundlæggende rettigheder og frihedsrettigheder.

c) Inddrage relevante interessenter i drøftelser og aktiviteter, der har til formål at fremme det internationale samarbejde om håndhævelse af lovgivningen om beskyttelse af personoplysninger.

d) Fremme udveksling og dokumentation af lovgivning om beskyttelse af personoplysninger og praksis på området, herunder om kompetencekonflikter med tredjelande.

Af forordningens præambelbetragtning nr. 116 fremgår det endvidere, at når personoplysninger overføres på tværs af grænser uden for Unionen, kan det medføre yderligere risici for fysiske personers mulighed for at udøve deres databeskyttelsesrettigheder og beskytte sig mod ulovlig brug eller videregivelse af disse oplysninger. Det fremgår desuden af betragtningen, at tilsynsmyndighederne samtidig i nogle tilfælde må konstatere, at de er ude af stand til at følge op på klager eller foretage undersøgelser vedrørende aktiviteter uden for deres grænser. Herudover fremgår det af betragtningen, at samarbejdet på tværs af grænserne også kan hæmmes af utilstrækkelige forebyggende eller afhjælpende beføjelser, uensartede retlige ordninger og praktiske hindringer som f.eks. ressourcebegrænsninger. Det fremgår endvidere af betragtningen, at der derfor er behov for at fremme tættere samarbejde mellem datatilsynsmyndigheder, så de bedre kan udveksle oplysninger og gennemføre undersøgelser sammen med de tilsvarende internationale organer. Endelig fremgår det af betragtningen, at med henblik på at udvikle mekanismer for internationalt samarbejde for at lette og yde international gensidig bistand til håndhævelsen af lovgivning om beskyttelse af personoplysninger bør Kommissionen og tilsynsmyndighederne udveksle oplys-

ninger og samarbejde om aktiviteter i forbindelse med udøvelsen af deres beføjelser med de kompetente myndigheder i tredjelande på grundlag af gensidighed og i overensstemmelse med denne forordning.

6.7.4. Overvejelser

Med databeskyttelsesforordningens artikel 50 forpligtes EU-Kommissionen og tilsynsmyndighederne til at træffe "de nødvendige foranstaltninger" med henblik på at samarbejde med tredjelande og internationale organisationer om beskyttelse af personoplysninger.

Det er umiddelbart svært at sige noget specifikt om rækkevidden af den forpligtelse, som EU-Kommissionen og tilsynsmyndighederne pålægges med den nye bestemmelse i databeskyttelsesforordningens artikel 50. Der er imidlertid næppe tvivl om, at bestemmelsen vil indebære, at tilsynsmyndigheder vil være nødt til at engagere sig yderligere i denne form for internationalt samarbejde.

Bestemmelsen indebærer dog næppe, at tilsynsmyndighederne vil være nødt til at deltage i alle internationale samarbejder om beskyttelse af personoplysninger. Derimod må bestemmelsen indeholde rum for, at tilsynsmyndighederne kan foretage en konkret vurdering af, hvorvidt man ønsker at tiltræde et givent samarbejde, herunder bl.a. under hensyn til samarbejdets opbygning, effektivitet og det medfølgende ressourceforbrug.

Det må også forventes, at det kommende Databeskyttelsesråd – eventuelt repræsenteret ved såkaldte undergrupper eller lignende – vil engagere sig i det internationale samarbejde om beskyttelse af personoplysninger, jf. herved databeskyttelsesforordningens artikel 70, stk. 1, litra v og w. Med de nye bestemmelser i artikel 70, stk. 1, litra v og w, vil arbejdet ikke længere være begrænset til at komme med udtalelser til EU-Kommissionen om beskyttelsesniveauet i tredjelande, jf. forordningens artikel 70, stk. 1, litra s. Tilsynsmyndighederne vil derfor formentlig også i et vist omfang kunne leve op til sine nye forpligtelser efter databeskyttelsesforordningens artikel 50 ved at deltage aktivt i Databeskyttelsesrådets internationale arbejde.

7. Forordningens kapitel VI: Uafhængige tilsynsmyndigheder

7.1. Tilsynsmyndighed, artikel 51, 53 og 54

7.1.1. Præsentation

I EU-Kommissionens meddelelse til Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget fra 2010[739] udtalte Kommissionen bl.a., forud for sit forslag til databeskyttelsesforordning fra 2012,[740] at gennemførelsen og håndhævelsen af databeskyttelsesprincipper og -regler er afgørende for at sikre overholdelse af fysiske personers rettigheder. I den sammenhæng spiller databeskyttelsesmyndighederne ifølge Kommissionen en særdeles vigtigt rolle i håndhævelsen af databeskyttelsesreglerne. De er uafhængige vogtere af de grundlæggende rettigheder og frihedsrettigheder med relation til beskyttelse af personoplysninger, og fysiske personer er afhængige af, at disse myndigheder sikrer, at deres personoplysninger beskyttes, og at databehandlingen foregår lovligt. Derfor finder Kommissionen, at deres rolle bør styrkes, ikke mindst i lyset af EU-Domstolens seneste retspraksis vedrørende deres uafhængighed,[741] og de bør have de nødvendige beføjelser og ressourcer, således at de på forsvarlig vis kan varetage deres opgaver både nationalt og i samarbejde med andre nationale databeskyttelsesmyndigheder.

EU's charter om grundlæggende rettigheder fastslår i den forbindelse også i artikel 8, stk. 3, at overholdelsen af chartrets artikel 8, stk. 1 og 2, om retten til beskyttelse af personoplysninger er underlagt en uafhængig myndigheds kontrol.

I modsætning til i dag, hvor chartret ikke angiver noget om, hvorledes dette tilsyn skal organiseres og varetage disse opgaver, og hvor man i databeskyttelsesdirektivet kun har medtaget én artikel om tilsynsmyndigheden, indeholder databeskyttelsesforordningen hele to kapitler om tilsynsmyndigheden og forpligtelse til at samarbejde og sikre sammenhæng (kapitel VI og VII). Forordningens kapitel VI, der har overskriften "Uafhængige tilsynsmyndigheder", består af 8 artikler og er delt op i to afdelinger. Første afdeling omhandler tilsynsmyndighedernes uafhængige status (artikel 51-54). Anden afdeling vedrører tilsynsmyndighedernes kompetence, opgaver og beføjelser (artikel 55-59).

[739] KOM (2010) 609 endelig, s. 18.
[740] EU-Kommissionens forslag af 25. januar 2013 (KOM (2012) 11 endelig).
[741] Se bl.a. EU-Domstolens dom af 9.3.2010, Kommissionen mod Tyskland, sag C-518/07 og EU-Domstolens dom af 6. oktober 2015, Maximillian Schrems mod det irske datatilsyn, sag C-362/14.

7.1.2. Gældende ret

7.1.2.1. Tilsynsmyndighedens udpegning og organisering

Databeskyttelsesdirektivet stiller i artikel 28, stk. 1, 1. afsnit, krav om, at hver medlemsstat skal drage omsorg for, at der *udpeges* en eller flere offentlige myndigheder, der har til opgave på dens område at påse overholdelsen af de bestemmelser, medlemsstaten vedtager til gennemførelse af dette direktiv.

Af databeskyttelsesdirektivets præambelbetragtning nr. 62 fremgår endvidere, at oprettelsen af en uafhængig tilsynsmyndighed i hver medlemsstat har afgørende betydning for beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger.

Direktivets artikel 28, stk. 1, er gennemført i dansk ret ved persondatalovens § 55, stk. 1, hvoraf det følger, at Datatilsynet, der består af et råd og et sekretariat, fører tilsyn med enhver behandling, der omfattes af loven, jf. dog kapitel 17.

Datatilsynet har som udgangspunkt kompetence over for enhver behandling, som omfattes af loven, jf. herved reglerne i lovens kapitel 1 om lovens område og kapitel 3 om lovens geografiske område. I persondatalovens kapitel 17 (§§ 67 og 68) er fastsat regler om, hvilken tilsynsmyndighed, der skal føre tilsyn med domstolenes behandling af personoplysninger, og om hvilke opgaver der henhører under vedkommende tilsynsmyndighed.

Af lovens § 67, stk. 1, fremgår, at Domstolsstyrelsen fører tilsyn med behandling af oplysninger, der foretages for domstolene. Tilsynet omfatter ifølge stk. 2, behandling af oplysninger med hensyn til domstolenes administrative forhold. For anden behandling af oplysninger træffes afgørelse af vedkommende ret, jf. § 67, stk. 3. Afgørelsen kan kæres til højere ret. For særlige domstole, hvis afgørelser ikke kan indbringes for højere ret, kan den i 1. pkt. nævnte afgørelse, kæres til den landsret, i hvis kreds retten er beliggende. Kærefristen er 4 uger fra den dag, afgørelsen er meddelt den pågældende.

Det fremgår i den forbindelse af Registerudvalgets betænkning nr. 1345, at databeskyttelsesdirektivet ikke kan antages at stille krav om koordinering mellem flere nationale tilsynsmyndigheder. Efter udvalgets opfattelse vil det imidlertid være hensigtsmæssigt, at der sker en sådan koordinering mellem Datatilsynet og Domstolsstyrelsen.[742]

Dette er baggrunden for, at det af persondatalovens § 66 fremgår, at Datatilsynet og Domstolsstyrelsen samarbejder, i det omfang det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle relevante oplysninger.

[742] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 370.

Det er i bemærkningerne til persondataloven forudsat, at tilsynsmyndighederne indbyrdes drøfter spørgsmål af mere principiel karakter, således at der sker den fornødne koordinering tilsynsmyndighederne imellem. Formålet er at sikre, at tilsynsmyndighedernes praksis ikke udvikler sig i forskellige retning.[743]

Det kan endvidere i lovgivningen være bestemt, at tilsynet med behandlingen af personoplysninger hører under andre myndigheder. I persondataloven med kommentarer er Sundhedsvæsenets Disciplinærnævn, Finanstilsynet, Forbrugerombudsmanden og Erhvervsstyrelsen medtaget som eksempler herpå.[744] I forhold til disse andre "tilsynsmyndigheder" foregår der i dag – på ulovbestemt grundlag – også en vis koordinering tilsynsmyndighederne imellem.

Databeskyttelsesdirektivet indeholder ikke regler om tilsynsmyndighedens nærmere organisering eller en opregning af, hvilke generelle betingelser der gælder i forhold til eventuelle "medlemmer" af en tilsynsmyndighed. Der er således i direktivet hverken medtaget regler om, hvordan udpegningen skal foregå, eller regler for, hvilke kvalifikationer hvert medlem skal være i besiddelse af, ligesom direktivet heller ikke forholder sig til, hvornår et medlems hverv ophører, herunder i hvilke situationer et medlem vil kunne afskediges.

Det fremgår imidlertid af persondatalovens § 55, stk. 2, at Datatilsynets daglige forretninger varetages af sekretariatet, der ledes af en direktør. Af bemærkningerne til persondataloven fremgår det endvidere, at sekretariatet forudsættes sammensat således, at det besidder såvel juridisk som edb-teknisk sagkundskab.[745]

Datarådet, der som nævnt ovenfor sammen med sekretariat udgør myndigheden Datatilsynet, nedsættes ifølge lovens § 55, stk. 3, af justitsministeren. Af denne bestemmelse fremgår endvidere, at rådet består af en formand, der er dommer, og af 6 andre medlemmer. Der kan udnævnes stedfortrædere for medlemmerne. Medlemmerne og stedfortræderne for disse udnævnes for 4 år (med mulighed for genbeskikkelse). Det bemærkes, at muligheden for at udpege stedfortrædere for medlemmerne af rådet, indtil videre ikke er udnyttet.

Det fremgår i den forbindelse af forarbejderne til § 55, stk. 3, at der ved udpegning af medlemmer af rådet skal tilstræbes uvildighed og sagkundskab og ikke interessere repræsentation. Rådets medlemmer skal derfor udpeges på en sådan måde, at der sikres Datatilsynet den fornødne uafhængighed af interesser inden for den offentlige forvaltning og private sektor.

[743] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 66.
[744] For nærmere se Persondataloven med kommentarer (2015), s. 617-618.
[745] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 55.

Samtidig er det anset for at være af afgørende betydning for Datatilsynets autoritet, at der blandt rådets medlemmer findes personer med betydelig indsigt i den offentlige (statslige såvel som kommunale) forvaltnings og erhvervslivets og arbejdsmarkedets forhold, da dette vil være en forudsætning for, at tilsynet kan foretage en selvstændig vurdering af de synspunkter, der kan anføres for og imod ønsker om påbegyndelsen og tilrettelæggelsen af bestemte behandlinger. Endelig er det i lovens forarbejder forudsat, at mindst ét medlem af rådet besidder indgående kendskab til informationsteknologi.

Rådets formand skal være dommer, og siden nedsættelsen af Registerrådet pr. 1. januar 1979 har formandsposten være beklædt af en højesteretsdommer. I forarbejderne forudsættes det, at denne praksis – på grund af Datatilsynets særlige funktion og status – i videst muligt omfang opretholdes.

Rådet fastsætter sin forretningsorden og de nærmere regler om arbejdets fordeling mellem råd og sekretariat jf. lovens § 55, stk. 4. Dette er sket ved bekendtgørelse nr. 1178 af 15. december 2000 om forretningsorden for Datarådet.

7.1.2.2. Tavshedspligt

Efter databeskyttelsesdirektivets artikel 28, stk. 7, skal medlemsstaterne fastsætte bestemmelser om, at tilsynsmyndighedernes medlemmer og ansatte også efter deres aktiviteters ophør har tavshedspligt, for så vidt angår de fortrolige oplysninger, de har adgang til.

Af Registerudvalgets betænkning nr. 1345 fremgår det, at efter forvaltningslovens § 27, stk. 1, har den, der virker inden for den offentlige forvaltning, tavshedspligt, jf. straffelovens § 152 og §§ 152 c - 152 f, når en oplysning ved lov eller anden gyldig bestemmelse er betegnet som fortrolig, eller når det i øvrigt er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til offentlige eller private interesser.[746] Dette gælder bl.a. for at varetage væsentlige hensyn til bl.a. enkeltpersoners interesse i at beskytte oplysninger om deres personlige eller interne, herunder økonomiske, forhold, samt enkeltpersoners økonomiske interesse i at beskytte oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold, jf. § 27, stk. 1, nr. 6 og 7. Endvidere straffes efter straffelovens § 152, stk. 1, den, som virker eller har virket i offentlig tjeneste eller hverv, og som uberettiget videregiver eller udnytter fortrolige oplysninger, hvortil den pågældende i den forbindelse har fået kendskab. Der var derfor efter udvalgets opfattelse ikke behov for særlige bestemmelser om tavshedspligt for ansatte mv. i tilsynet i en ny kommende lovgivning.

[746] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 358.

Ansatte i Datatilsynet er på den baggrund i dag ikke underlagt en særlig tavshedspligt, men den almindelige tavshedspligt for offentlige ansatte.

Endelig skal det bemærkes, at der for Finanstilsynets ansatte gælder 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.

7.1.3. Databeskyttelsesforordningen

7.1.3.1. Tilsynsmyndighed

7.1.3.1.1. Databeskyttelsesforordningens artikel 51, stk. 1

Af databeskyttelsesforordningens artikel 51, stk. 1, fremgår det, at hver medlemsstat sikrer, at en eller flere uafhængige offentlige myndigheder er ansvarlige for at føre tilsyn med anvendelsen af denne forordning, for at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling og for at lette fri udveksling af personoplysninger i Unionen ("tilsynsmyndighed").

Det fremgår endvidere af databeskyttelsesforordningens præambelbetragtning nr. 117, 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.

7.1.3.1.2 Databeskyttelsesforordningens artikel 51, stk. 2

Efter forordningens artikel 51, stk. 2, bidrager hver enkelt tilsynsmyndighed til ensartet anvendelse af denne forordning i hele Unionen. Til dette formål samarbejder tilsynsmyndighederne med hinanden og med Kommissionen i henhold til kapitel VII.

7.1.3.1.3 Databeskyttelsesforordningens artikel 51, stk. 3

Hvis der er mere end én tilsynsmyndighed i en medlemsstat, udpeger den pågældende medlemsstat ifølge forordningens artikel 51, stk. 3, en tilsynsmyndighed, der skal repræsentere disse myndigheder i Databeskyttelsesrådet, og fastsætter en mekanisme, som sikrer, at de andre myndigheder overholder reglerne vedrørende den sammenhængsmekanisme, der er omhandlet i artikel 63.

Herom er det videre i forordningens præambelbetragtning nr. 119 anført, at hvis en medlemsstat opretter flere tilsynsmyndigheder, bør den ved lov fastlægge mekanismer, der sikrer disse tilsynsmyndig-heders effektive deltagelse i sammenhængsmekanismen. Den

pågældende medlemsstat bør navnlig udpege den tilsynsmyndighed, der fungerer som fælles kontaktpunkt for disse myndigheders effektive deltagelse i mekanismen, med henblik på at sikre et hurtigt og smidigt samarbejde med andre tilsynsmyndigheder, Databeskyttelsesrådet og Kommissionen.

7.1.3.1.4. Databeskyttelsesforordningens artikel 51, stk. 4

Af forordningens artikel 51, stk. 4, fremgår, at hver medlemsstat senest den 25. maj 2018 skal give Kommissionen meddelelse om de bestemmelser, som den vedtager i henhold til dette kapitel, og underretter den straks om alle senere ændringer, der berører dem.

7.1.3.2. Generelle betingelser for medlemmer af en tilsynsmyndighed (artikel 53)

7.1.3.2.1. Databeskyttelsesforordningens artikel 53, stk. 1

Det fremgår af forordningens artikel 53, stk. 1, at medlemsstaterne sikrer, at hvert medlem af en tilsynsmyndighed udnævnes efter en gennemsigtig procedure af enten deres parlament, deres regering, deres statschef, eller et uafhængigt organ, der i henhold til medlemsstaternes nationale ret har fået overdraget ansvaret for udnævnelsen.

Endvidere fremgår det af præambelbetragtning nr. 121, at de generelle betingelser for en tilsynsmyndigheds medlem eller medlemmer bør fastsættes ved lov i hver medlemsstat og det bør navnlig fastsættes, at disse medlemmer skal udnævnes ved en gennemsigtig procedure enten af parlamentet, regeringen eller statschefen i den pågældende medlemsstat på grundlag af et forslag fra regeringen, et medlem af regeringen, parlamentet eller et kammer i parlamentet eller af et uafhængigt organ, der har bemyndigelse hertil i henhold til medlemsstaternes nationale ret.

Databeskyttelsesforordningens artikel 53, stk. 1, fastslår således, at udnævnelsen af hvert medlem af en tilsynsmyndighed skal ske efter en gennemsigtig procedure, der skal fremgå af de enkelte medlemsstaters lovgivning.

Forordningen indeholder ikke nogen nærmere definition af, hvad der nærmere forstås ved udtrykket en tilsynsmyndigheds ”medlem eller medlemmer”. Af forordningens artikel 54, stk. 1, litra f, må imidlertid kunne udledes, at ”medlem eller medlemmer” ikke er det samme som personale, idet ordet ”personale” fremgår af denne bestemmelse ved siden af ordene ”medlem og medlemmer”.

Den samme skelnen mellem ”medlem og medlemmer” og ”personale” fremgår også af artikel 54, stk. 2, vedrørende tavshedspligt.

Som et andet fortolkningsbidrag kan endvidere henvises til næstsidste punktum i præambelbetragtning nr. 129. Det fremgår heraf, at hver juridisk bindende foranstaltning, der træffes af en tilsynsmyndighed, bør være skriftlig, klar og utvetydig, angive navnet på den tilsynsmyndighed, der har truffet foranstaltningen, og datoen for iværksættelse af foranstaltningen, *være underskrevet af chefen for eller et medlem af tilsynsmyndigheden, som vedkommende har givet bemyndigelse hertil*, angive begrundelsen for foranstaltningen og indeholde en henvisning til adgang til effektive retsmidler.

Om der i en tilsynsmyndighed vil være et eller flere medlemmer afhænger således i sidste ende af, hvilken konstruktion, der vælges for tilsynsmyndigheden.

7.1.3.2.2. Databeskyttelsesforordningens artikel 53, stk. 2
Af databeskyttelsesforordningens artikel 53, stk. 2, fremgår det, at hvert medlem skal have de kvalifikationer, den erfaring og den kompetence, navnlig på området beskyttelse af personoplysninger, der er nødvendige for at varetage dets hverv og udøve dets beføjelser.

7.1.3.2.3. Databeskyttelsesforordningens artikel 53, stk. 3 og 4
Det fremgår af forordningens artikel 53, stk. 3, at et medlems hverv ophører ved udløbet af embedsperioden, ved frivillig fratrædelse eller ved obligatorisk fratrædelse i overensstemmelse med den pågældende medlemsstats nationale ret.

Endvidere fremgår det af databeskyttelsesforordningens artikel 53, stk. 4, at et medlem kun må afskediges i tilfælde af alvorligt embedsmisbrug, eller hvis medlemmet ikke længere opfylder betingelserne for at varetage sit hverv.

7.1.3.3. Regler om oprettelse af en tilsynsmyndighed (artikel 54)
7.1.3.3.1. Databeskyttelsesforordningens artikel 54, stk. 1
Af forordningens artikel 54, stk. 1, fremgår det, at hver medlemsstat ved lov fastsætter følgende:

a) den enkelte tilsynsmyndigheds oprettelse

b) de nødvendige kvalifikationer og udvælgelseskriterier, der skal være opfyldte for at kunne blive udnævnt til medlem af den enkelte tilsynsmyndighed

c) reglerne og procedurerne for udnævnelse af medlemmet eller medlemmerne af den enkelte tilsynsmyndighed

d) embedsperioden for medlemmer eller medlemmerne af den enkelte tilsynsmyndighed på mindst fire år med undtagelse af den første udnævnelse efter den 24. maj 2016, som kan være af kortere varighed, hvis det er nødvendigt for at beskytte den pågældende tilsynsmyndighed uafhængighed ved hjælp af en forskudt udnævnelsesprocedure

e) om og i bekræftende fald for hvor mange embedsperioder medlemmet eller medlemmerne af den enkelte tilsynsmyndighed kan genudnævnes

f) betingelserne vedrørende forpligtelser for den enkelte tilsynsmyndigheds medlem eller medlemmer og personale, forbud mod handlinger, hverv og fordele, der er uforenelige hermed, under og efter embedsperioden, og regler for arbejdsophør.

Endvidere fremgår det af præambelbetragtning nr. 121, at de generelle betingelser for en tilsynsmyndigheds medlem eller medlemmer bør fastsættes ved lov i hver medlemsstat og navnlig bør fastsætte, at disse medlemmer skal udnævnes ved en gennemsigtig procedure enten af parlamentet, regeringen eller statschefen i den pågældende medlemsstat på grundlag af et forslag fra regeringen, et medlem af regeringen, parlamentet eller et kammer i parlamentet eller af et uafhængigt organ, der har bemyndigelse hertil i henhold til medlemsstaternes nationale ret.

Herudover fremgår det af præambelbetragtning nr. 121, at for at sikre tilsynsmyndighedens uafhængighed bør medlemmet eller medlemmerne handle med integritet, afholde sig fra enhver handling, der er uforenelig med deres hverv, og ikke, så længe deres embedsperiode varer, udøve uforenelig lønnet eller ulønnet virksomhed. Tilsynsmyndigheden bør have sit eget personale, der er udvalgt af tilsynsmyndigheden eller et uafhængigt organ, der er oprettet ved medlemsstaternes nationale ret, og som udelukkende bør være underlagt tilsynsmyndighedens medlems eller medlemmers ledelse.

7.1.3.3.2 Databeskyttelsesforordningens artikel 54, stk. 2.

Det fremgår af forordningens artikel 54, stk. 2, at den enkelte tilsynsmyndigheds medlem eller medlemmer og personale i overensstemmelse med EU-retten eller medlemsstaternes nationale ret såvel under som efter deres embedsperiode har tavshedspligt for så vidt angår alle fortrolige oplysninger, der er kommet til deres kendskab under udførelsen af deres opgaver eller udøvelsen af deres beføjelser. I deres embedsperiode gælder denne tavshedspligt især indberetninger fra fysiske personer af overtrædelser af denne forordning.

Dette svarer til, hvad der er gældende ret i dag.

7.1.4. Overvejelser

Databeskyttelsesforordningens artikel 51, stk. 1, svarer i det store hele til artikel 28, stk. 1, i databeskyttelsesdirektivet. Det vil således også i tiden efter, at forordningen finder anvendelse fra den 25. maj 2018 være muligt at opretholde den nuværende danske tilsynsmodel på databeskyttelsesområdet, hvor Datatilsynet og Domstolsstyrelsen er de uafhængige myndigheder, der fører tilsyn med, at reglerne i persondataloven overholdes.

Nyt er det imidlertid, at oprettelsen af en eller flere tilsynsmyndigheder forudsætter vedtagelse af lovregler, jf. forordningens artikel 51, stk. 4. Efter databeskyttelsesdirektivet er det alene et krav, at der udpeges en eller flere tilsynsmyndigheder. Det fremgår endvidere, hvordan denne udpegning skal foregå, herunder om det kræver vedtagelse af regler, eller om det er nok, at udpegningen sker ved en (intern) regeringsbeslutning.

Den ændrede retstilstand får dog ikke nogen nævneværdig betydning herhjemme, da det i Danmark allerede er normal praksis, når der oprettes (offentlige) myndigheder mv., at gøre dette ved lov eller i medfør af lov. Reglerne om tilsynsmyndigheden må dog forventes at blive noget mere detaljerede. Dette gælder ikke mindst, når henses til den ganske detaljerede regulering i forordningens artikel 53 og artikel 54 om det enkelte medlem eller medlemmerne af tilsynsmyndighed. Flere af betingelserne er dog allerede gældende ret i dag, jf. persondatalovens § 55 og forarbejderne hertil,

At tilsynsmyndighederne er forpligtet til at samarbejde med hinanden er ikke nyt, men samarbejdsforpligtelsen i forordningen er ny, og den har også fået en helt anden og langt mere fremtrædende rolle. Hvor forpligtelsen i databeskyttelsesdirektivet alene fremgår til sidst i et af de sidste stykker i den eneste bestemmelse om tilsynsmyndigheden, nævnes den således allerede nu i denne første bestemmelse i det nye kapitel i forordningen om de uafhængige tilsynsmyndigheder, jf. forordningens artikel 51, stk. 2.

Forpligtelsen i forordningens artikel 51, stk. 3, 1. led for den enkelte medlemsstat til - hvis der er mere end én tilsynsmyndighed i en medlemsstat, – at udpege en tilsynsmyndighed, der skal repræsentere disse myndigheder i Databeskyttelsesrådet, svarer til situationen efter gældende ret. Det er derimod nyt – og ikke uden videre nogen let opgave – når det i forordningens artikel 51, stk. 3, 2. led, fastslås, at der skal fastsættes en mekanisme, som sikrer, at de andre myndigheder overholder reglerne vedrørende den sammenhængsmekanisme, der er omhandlet i artikel 63.

7.2. Uafhængighed, artikel 52

7.2.1. Præsentation

I Danmark varetages tilsynet med behandling af personoplysninger af Datatilsynet, jf. persondatalovens § 55, stk. 1, og for behandling af personoplysninger, som foretages for domstolene, dels af Domstolsstyrelsen, jf. lovens § 67, stk. 1-2, og dels af vedkommende ret, jf. lovens § 67, stk. 3.

Ifølge persondatalovens § 56 (og henvisningen hertil i lovens § 68) udøver Datatilsynet og Domstolsstyrelsen deres funktioner i fuld uafhængighed.

Af betydning for uafhængigheden er den nærmere organisering, som for Datatilsynets vedkommende følger af persondatalovens § 55, mens organiseringen af Domstolsstyrelsen følger af reglerne i lov om Domstolsstyrelsen.[747]

Persondatalovens §§ 55-56 og §§ 67-68 gennemfører databeskyttelsesdirektivets artikel 28, stk. 1, som fastsætter, at medlemsstaterne skal udpege uafhængige tilsynsmyndigheder.

Som anført ovenfor under afsnit 7.1. fastsætter databeskyttelsesforordningens artikel 51 krav om tilsynsmyndigheder. Forordningens artikel 52 fastsætter krav til tilsynsmyndighedernes uafhængighed. Artikel 53-54 fastsætter endvidere generelle beføjelser for medlemmerne af en tilsynsmyndighed og regler for tilsynsmyndighedens oprettelse.

7.2.2. Gældende ret

7.2.2.1. Databeskyttelsesdirektivet artikel 28

Efter databeskyttelsesdirektivets artikel 28, stk. 1, drager hver medlemsstat omsorg for, at der udpeges en eller flere offentlige myndigheder, der har til opgave på dens område at påse overholdelsen af de bestemmelser, medlemsstaten vedtager til gennemførelse af databeskyttelsesdirektivet. Ifølge samme bestemmelse udøver disse myndigheder de funktioner, som de tillægges, i *fuld uafhængighed*.[748]

Ifølge databeskyttelsesdirektivets præambelbetragtning nr. 62, har oprettelsen af en uafhængig tilsynsmyndighed i hver medlemsstat afgørende betydning for beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger.

---

[747] Lov nr. 401 af 26. juni 1998 med senere ændringer.

[748] Kravet om en uafhængig tilsynsmyndigheds kontrol med overholdelsen af Unionens regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger fremgår også af den primære EU-ret, bl.a. artikel 8, stk. 3, i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 16, stk. 2, i Traktaten om Den Europæiske Unions Funktionsmåde.

Den nærmere fortolkning af uafhængighedskriteriet i direktivets artikel 28, stk. 1, er fastlagt af EU-Domstolen ved dom af 9. marts 2010 i sag C-518/07, Kommissionen mod Tyskland, ved dom af 16. oktober 2012 i sag C-614/10, Kommissionen mod Østrig samt ved dom af 8. april 2014 i sag C-288/12, Kommissionen mod Ungarn.

I sag C-518/07 fandt EU-Domstolen, at Tyskland havde tilsidesat sine forpligtelser ved at have underlagt de nationale tilsynsmyndigheder, der var kompetente med hensyn til behandling af personoplysninger uden for den offentlige sektor i de forskellige delstater, et statsligt tilsyn og således foretaget en ukorrekt gennemførelse af kravet om »fuld uafhængighed« for de myndigheder, der skal sikre beskyttelsen af disse oplysninger.

Om rækkevidden af kravet om fuld uafhængighed udtalte EU-Domstolen generelt i præmis 18, at udtrykket 'uafhængighed' normalt betegner en status, som sikrer, at det pågældende organ kan handle helt frit uden nogen form for instruks eller pression. Domstolen udtalte endvidere, at udtrykket 'fuld uafhængighed' indebærer en beslutningsbeføjelse for tilsynsmyndigheden, der er unddraget enhver ydre påvirkning, hvad enten denne er direkte eller indirekte.[749]

EU-Domstolen udtalte yderligere i præmis 25, at formålet med tilsynsmyndighedernes uafhængighed er at sikre et effektivt og pålideligt tilsyn med overholdelsen af reglerne om beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger, og at uafhængigheden skal fortolkes i lyset af dette formål. EU-Domstolen udtalte tillige, at tilsynsmyndighedernes uafhængighed ikke er etableret med henblik på at give disse myndigheder og deres ansatte en særlig status, men med henblik på at styrke beskyttelsen af personer og organer, der måtte blive berørt af deres afgørelser, og at det følger heraf, at når tilsynsmyndighederne udøver deres funktioner, skal de handle objektivt og upartisk. Derfor skal de beskyttes imod enhver form for ydre påvirkning, herunder direkte eller indirekte påvirkning fra staten eller delstaterne, og ikke blot imod påvirkning fra de kontrollerede organer.

Ydermere udtalte EU-Domstolen i præmis 28, at tilsynsmyndighedernes uafhængighed forudsætter, at udøvelsen af deres funktioner ikke er underlagt nogen instrukser.

Sammenfattende om rækkevidden af uafhængighedskriteriet udtalte EU-Domstolen i præmis 30, at de tilsynsmyndigheder, der er kompetente med hensyn til behandling af personoplysninger uden for den offentlige sektor, skal være uafhængige, således at de har mulighed for at udøve deres funktioner uden ydre påvirkning, og at denne uafhængighed ikke

[749] Præmis 18-19.

alene udelukker enhver påvirkning, der bliver udøvet af de kontrollerede organer, men også ethvert påbud og enhver anden ydre påvirkning — hvad enten denne er direkte eller indirekte — der kan skabe tvivl om udførelsen af de nævnte myndigheders opgave, der består i at skabe en ligevægt mellem beskyttelsen af retten til privatlivets fred og den frie udveksling af personoplysninger.

Om den konkrete sag anførte EU-Domstolen i præmis 32, at det statslige tilsyn gav mulighed for, at den pågældende regering eller et administrativt organ, der er underlagt denne regering, kunne øve direkte eller indirekte indflydelse på tilsynsmyndighedernes beslutninger eller i givet fald annullere eller erstatte disse beslutninger.

I forlængelse heraf anførte EU-Domstolen i præmis 34, at det ikke kunne udelukkes, at tilsynsmyndighederne, der indgår i den almindelige forvaltning, og som derfor er underlagt regeringen, ikke er i stand til at handle på en objektiv måde, når de fortolker og anvender bestemmelserne om behandling af personoplysninger. Om den omstændighed, at der var tale om et statsligt tilsyn for tilsynsmyndigheder, der fører tilsyn uden for den offentlige sektor, henviste EU-Domstolen i præmis 35 til, at den pågældende regering kan have interesse i ikke at overholde bestemmelserne om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, når der er tale om et ikke-offentligt organs behandling af sådanne oplysninger. Denne regering kan selv være berørt af denne behandling, hvis den deltager heri eller ville kunne deltage heri, f.eks. i tilfælde af offentlig-private partnerskaber eller i forbindelse med offentlige kontrakter med den private sektor. Regeringen kan også have en særlig interesse, hvis det er nødvendigt eller endog blot nyttigt for den at få adgang til databaser for at udføre sine opgaver bl.a. med skattemæssige formål eller retshåndhævelsesformål for øje. Selv samme regering kan i øvrigt også være tilbøjelig til at foretrække at fremme økonomiske interesser, når virksomheder, der i økonomisk henseende er vigtige for staten eller regionen, anvender de nævnte bestemmelser.

EU-Domstolen bemærkede i præmis 36, at foreligger der blot en risiko for, at det statslige tilsyn kan øve politisk indflydelse på tilsynsmyndighedernes beslutninger, er dette tilstrækkeligt til at hindre, at sidstnævnte kan udøve deres opgaver uafhængigt, hvilket for det første kan medføre en forudgående lydighed fra disse myndigheders side over for det statslige tilsyns beslutningspraksis, og for det andet kræver den rolle som vogter af retten til privatlivets fred, som tilsynsmyndigheden har påtaget sig, at deres beslutninger og således myndigheden selv står uden for enhver mistanke om partiskhed.

EU-Domstolen kom på den baggrund frem til, at det statslige tilsyn i Tyskland ikke var foreneligt med kravet om uafhængighed, jf. præmis 37.

På baggrund af at Tyskland havde rejst spørgsmål om forholdet til en række demokratiske principper, udtalte EU-Domstolen i øvrigt i præmis 43-46, at databeskyttelsesdirektivet ikke på nogen måde pålægger medlemsstaterne at holde disse [tilsyns-]myndigheder uden for enhver parlamentarisk indflydelse, og at de personer, der påtager sig ledelsen af tilsynsmyndighederne, således kan udpeges af parlamentet eller regeringen, ligesom parlamentet kan fastlægge de nævnte myndigheders beføjelser og forpligtelser til f.eks. at rapportere om deres aktiviteter til parlamentet, samt at uafhængighed af den almindelige forvaltning ikke i sig selv fratager disse myndigheders demokratiske legitimitet.

I sag C-614/10 fandt EU-Domstolen, at Østrig havde tilsidesat sine forpligtelser ved at have indført retsforskrifter, hvorefter det administrerende medlem af tilsynsmyndigheden (Datenschutzkommission), som bestod af seks medlemmer, var en statstjenestemand undergivet et tjenstligt tilsyn fra forbundskansleren, tilsynsmyndighedens kontor var en integreret del i forbundskanslerens tjenestegrene, og forbundskansleren havde en ubetinget ret til at blive informeret om alle aspekter ved forvaltningen af tilsynsmyndigheden.

I præmis 41 udtalte EU-Domstolen generelt under henvisning til dommen i sag C-518/07[750], at databeskyttelsesdirektivet skal fortolkes således, at tilsynsmyndighederne, der er kompetente med hensyn til behandling af personoplysninger, skal være uafhængige, således at de har mulighed for at udøve deres funktioner uden direkte eller indirekte udefrakommende påvirkning, som vil kunne påvirke deres afgørelser.

For så vidt angår det tjenstlige tilsyn for det administrerende medlem i den konkrete sag udtalte EU-Domstolen i præmis 42, at funktionel uafhængighed ved, at tilsynsmyndighedens medlemmer i medfør af østrigsk ret er uafhængige og ikke er bundet af nogen instrukser i udøvelsen af deres hverv, er en nødvendig betingelse for at kunne leve op til uafhængighedskriteriet, men at dette ikke i sig selv er tilstrækkeligt til at sikre myndigheden mod enhver udefrakommende påvirkning.

I forlængelse heraf udtalte EU-Domstolen generelt i præmis 43, at databeskyttelsesdirektivets artikel 28, stk. 1, ikke alene har til formål at udelukke direkte indflydelse i form af instrukser, men også enhver form for indirekte indflydelse, der vil kunne påvirke tilsynsmyndighedernes afgørelser.

Endvidere udtalte EU-Domstolen om den konkrete sag i præmis 50, at henset til den stilling, som det administrerende medlem indtog i tilsynsmyndigheden, kunne medlemmets

[750] Præmis 19, 25, 30 og 50.

direkte foresattes tilsynsbeføjelser gribe ind i tilsynsmyndighedens uafhængighed ved udøvelsen af myndighedens funktioner.

I forlængelse heraf bemærkede EU-Domstolen i præmis 51-52, at det ikke kunne udelukkes, at den direkte foresattes vurdering af det administrerende medlem med henblik på at fremme nævnte tjenestemands fremgang ville kunne føre til en form for forudgående lydighed hos medlemmet, og at det på grund af forholdet mellem det administrerende medlem og det politiske organ, som myndigheden fører tilsyn med, ikke er hævet over enhver mistanke om partiskhed, som krævet efter artikel 28, stk. 1, i direktivet.

Om den omstændighed, at tilsynsmyndigheden var en integreret del i forbundskanslerens tjenestegrene udtalte EU-Domstolen i præmis 57, at dette ikke tillod den slutning, at tilsynsmyndigheden kunne udøve sine funktioner uden enhver påvirkning fra forbundskanslerens kontor.

Herom udtalte EU-Domstolen endvidere mere generelt i præmis 58, at tilsynsmyndigheden ganske vist ikke har brug for en selvstændig budgetpost for at kunne opfylde uafhængighedskriteriet, og at det dermed kan bestemmes, at tilsynsmyndigheden i budgetmæssig henseende henhører under et bestemt ministerområde, men at tildeling af udstyr og personalemæssige ressourcer, som er nødvendige for en sådan myndighed, ikke må forhindre den i at udøve sine funktioner i fuld uafhængighed.

Endvidere anførte EU-Domstolen om integreringen i forbundskanslerens tjenestegrene i præmis 61, at det under hensyn til arbejdsbyrden for en tilsynsmyndighed på den ene side og den omstændighed, at medlemmerne af tilsynsmyndigheden i medfør af østrigsk lovgivning udførte deres opgaver ved siden af andre erhvervsmæssige aktiviteter, på den anden side, måtte antages, at medlemmerne af en sådan myndighed i vidt omfang baserer udøvelsen af deres opgaver på bistand fra ansatte, som er stillet til deres rådighed. Den omstændighed, at kontoret bestod af tjenestemænd i forbundskanslerens kontor, som selv var under tilsyn af tilsynsmyndigheden, indebar en risiko for, at der blev øvet indflydelse på sidstnævntes afgørelser. Under alle omstændigheder var en så tæt organisatorisk sammenknytning mellem tilsynsmyndigheden og forbundskanslerens kontor til hinder for, at tilsynsmyndigheden var hævet over enhver mistanke om partiskhed, og følgelig var det uforeneligt med kravet om »uafhængighed« som omhandlet i artikel 28, stk. 1, andet afsnit, i databeskyttelsesdirektivet.

Endelig udtalte EU-Domstolen i præmis 62-63 om forbundskanslerens ubetingede ret til at blive informeret af det administrerende medlem om alle aspekter ved forvaltningen af til-

synsmyndigheden, at en sådan ret kunne undergive tilsynsmyndigheden en indirekte indflydelse fra forbundskansleren, der var uforenelig med uafhængighedskriteriet.

I sag C-288/12 fandt EU-Domstolen, at Ungarn havde tilsidesat sine forpligtelser i henhold til databeskyttelsesdirektivet ved i forbindelse med en omstrukturering at have bragt tilsynsmyndighedens mandat til ophør før tid.

EU-Domstolen udtalte generelt om ophør af tilsynsmyndigheders mandat i præmis 54, at hvis en medlemsstat kunne bringe en tilsynsmyndigheds mandat til ophør før dets oprindeligt fastsatte udløb, uden at de regler og garantier, der er blevet opstillet med henblik herpå ved den gældende lovgivning, overholdes, ville truslen om et sådant ophør før tid, som en sådan myndighed ville blive udsat for i den periode, hvori den udøver sit mandat, kunne føre til en form for lydighed fra dennes side i forhold til den politiske magt, der er uforenelig med det nævnte krav om uafhængighed. Endvidere anførte Domstolen herom, at dette gælder, selv når mandatets ophør før tid skyldes en omstrukturering eller en ændring af en udformning, idet sådanne omstruktureringer eller ændringer skal være organiseret på en sådan måde, at de krav om uafhængighed, der er opstillet i den gældende lovgivning, overholdes.

I forlængelse heraf udtalte EU-Domstolen i præmis 55, at artikel 28, stk. 1, i direktivet derfor nødvendigvis skal fortolkes således, at det omfatter forpligtelsen til at respektere tilsynsmyndighedernes mandats varighed indtil dettes udløb og til kun at lade dette mandat ophøre før tid i overensstemmelse med den gældende lovgivnings regler og garantier.

Endvidere udtalte EU-Domstolen i præmis 60, at medlemsstaterne kan vedtage og ændre den institutionelle udformning, som de anser for at være den mest egnede for deres tilsynsmyndigheder, men at de imidlertid inden for denne ramme skal sikre sig, at de ikke bringer kontrolmyndighedens uafhængighed i fare, hvilket omfatter forpligtelsen til at respektere varigheden af myndighedens mandat i overensstemmelse med det nævnte i præmis 54 nævnt ovenfor.

EU-Domstolen udtalte yderligere i præmis 61 om den omhandlede ungarske ændring, at den institutionelle udformning således ikke i sig selv objektivt kunne begrunde, at mandatet for den person, der var blevet tillagt funktionerne som tilsynsførende, blev bragt til ophør, uden at der blev fastsat overgangsforanstaltninger, der gjorde det muligt at sikre, at mandatets varighed blev overholdt.

7.2.2.2. Persondataloven

I Danmark er databeskyttelsesdirektivets artikel 28, stk. 1, bl.a. gennemført med oprettelsen af Datatilsynet som tilsynsmyndighed i medfør af persondatalovens § 55 og lovfæstelse af uafhængighedskriteriet i lovens § 56. For så vidt angår behandling af oplysninger for domstolene er det imidlertid dels Domstolsstyrelsen, dels vedkommende ret, der er udpeget som tilsyn, jf. persondatalovens § 67.[751]

7.2.2.2.1. Datatilsynet

Datatilsynet er således den uafhængige tilsynsmyndighed i Danmark, medmindre der er tale om behandling af personoplysninger for domstolene, jf. persondatalovens § 55, stk. 1.

Tilsynet udøver sine funktioner i fuld uafhængighed, jf. persondatalovens § 56.

Det fremgår af bemærkningerne til persondataloven, at det tidligere registertilsyn efter Registerudvalgets opfattelse levede op til kravet om fuld uafhængighed.[752] Tilsynet er den højeste administrative myndighed på området og udøver sine funktioner i fuld uafhængighed. Desuden har tilsynet en finanslovmæssig og personalemæssig tilknytning til Justitsministeriet, som er ressortministerium for lovgivningen, men tilsynet er under udførelsen af sine funktioner som tilsynsmyndighed ikke undergivet instruktionsbeføjelse af Justitsministeriet.

Endvidere fremgår det af Registerudvalgets betænkning, at det antages, at der i tilsynets fulde uafhængighed navnlig ligger, at myndighederne skal være funktionelt uafhængige og ikke må være undergivet instruktionsbeføjelse fra en anden myndighed. Det må antages, at det ville være i strid med direktivet, hvis en tilsynsmyndigheds afgørelser og udtalelser generelt kunne indbringes for en anden administrativ myndighed, f.eks. Justitsministeriet, medmindre der er tale om en egentlig klageinstans, som er funktionelt uafhængig.[753]

Det følger af persondatalovens § 55, stk. 1, at Datatilsynet består af et råd og et sekretariat.

Efter lovens § 55, stk. 2, varetages tilsynets daglige forretninger af sekretariatet, der ledes af en direktør, mens rådet, som nedsættes af justitsministeren, består af en formand, der er dommer, og af 6 andre medlemmer. Der kan udnævnes stedfortrædere for medlemmerne. Medlemmerne og stedfortræderne for disse udnævnes for 4 år. Rådet fastsætter sin egen forretningsorden og de nærmere regler om arbejdets fordeling mellem råd og sekretariat.

[751] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.8.2. og 4.2.8.3. i de almindelige bemærkninger.
[752] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, Afsnit 4.2.8.2.A. i de almindelige bemærkninger.
[753] Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 350 ff.

Om kernen i den tilsynsordning, som er videreført med Datatilsynet, fremgår det af bemærkningerne til persondataloven[754], at tilsynet består af et sekretariat, der varetager tilsynets daglige forretninger, og et råd, der navnlig behandler sager af principiel karakter. Det fremgår endvidere[755], at der ved udpegning af medlemmer af rådet skal tilstræbes uvildighed og sagkundskab, og at rådets medlemmer således skal udpeges på en sådan måde, at der sikres Datatilsynet den fornødne uafhængighed af interesser inden for den offentlige og private sektor. Endvidere fremgår det, at formandsposten hidtil (i Registertilsynet) havde været beklædt af en højesteretsdommer, og at denne praksis på grund af Datatilsynets særlige funktion og status i videst muligt omfang bør opretholdes. Desuden fremgår det i forhold til rådets fastsættelse af sin egen forretningsorden, at der vil kunne fastsættes nærmere regler om sagernes formelle behandling, herunder om, hvor mange medlemmer af rådet der skal være til stede, for at rådet kan anses for beslutningsdygtigt, om indkaldelse af stedfortræder osv. samt om, at visse typer af sager kan afgøres af sekretariatet på Datatilsynets vegne.

Det fremgår af Registerudvalgets betænkning, at det efter den dagældende lov om offentlige myndigheders registre § 25 var justitsministeren, som havde kompetence til at fastsætte Registerrådets forretningsorden, men at Registerudvalgets flertal var af den opfattelse, at Datarådet, som afløste Registerrådet, burde være kompetent til at fastsætte sin egen forretningsorden og de nærmere regler om arbejdets fordeling mellem råd og sekretariat.

7.2.2.2.2. Tilsynet med behandling af personoplysninger for domstolene

Ifølge persondatalovens § 67 føres tilsynet med domstolene i domstolsregi.

I den henseende har lovgiver fulgt hovedlinjerne i Registerudvalgets flertals anbefalinger til tilsynsordningen for domstolene.[756] Det fremgår af anbefalingerne, at hensynet til at gennemføre en så enstrenget tilsynsordning som muligt taler for at etablere en ordning, hvorefter tilsynet med domstolene i det hele placeres i domstolsregi, da det af principielle grunde ikke kunne anbefales, at Datatilsynet fører tilsyn med domstolenes judicielle funktioner, som også ifølge flertallet er bedst stemmende med grundlovens principper om domstolenes uafhængighed.

[754] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.8.2.A. i de almindelige bemærkninger.

[755] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 55.

[756] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.8.2. og 4.2.8.3. i de almindelige bemærkninger samt Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 374 ff.

Efter persondatalovens § 67, stk. 1, er det *Domstolsstyrelsen*, der fører tilsyn med behandling af oplysninger, der foretages for domstolene, jf. stk. 1. Tilsynet omfatter i medfør af bestemmelsens stk. 2 imidlertid kun behandling af oplysninger med hensyn til *domstolenes administrative forhold*.

Det fremgår af bemærkningerne til persondataloven[757], at Domstolsstyrelsens tilsyn således omfatter den teknisk-administrative behandling af oplysninger, herunder spørgsmålet om behandlingssikkerheden, hvilket bl.a. indebærer, at førelsen af en elektronisk oversigt over for de ved et embede ansatte personers forhold mv. er omfattet af tilsynet.

Endvidere fremgår det af bemærkningerne, at det tilsyn, som ifølge Registerudvalgets flertals anbefalinger skulle føres med domstolenes administrative funktioner, efter flertallets opfattelse i det væsentlige burde svare til, hvad der blev foreslået i relation til Datatilsynet, dog således at der på enkelte punkter burde fastsættes særlige regler for tilsynet på området. Det tilsyn, som skulle udføres, burde efter udvalgets opfattelse tilrettelægges således, at der træffes (bindende) afgørelse i forhold til den pågældende dataansvarlige domstol vedrørende dennes behandling af oplysninger.

Tilsynsmyndigheden burde herunder kunne træffe afgørelse om, at oplysninger skulle blokeres, slettes eller tilintetgøres, samt om, at det midlertidigt eller definitivt er forbudt at behandle nærmere angivne oplysninger. I overensstemmelse hermed blev det foreslået, at vedkommende tilsynsmyndighed i forbindelse med udførelsen af tilsynet skulle kunne træffe afgørelse vedrørende lovligheden mv. af den behandling af oplysninger, som fandt sted. Afgørelserne burde være endelige i den forstand, at der ikke kunne påklages til en højere administrativ myndighed. Derimod ville afgørelserne være undergivet domstolskontrol, jf. herved grundlovens § 63.[758]

Det bemærkes, at Registerudvalget i sin betænkning havde anbefalet, at det var vedkommende landsretspræsident og for Højesteret og Den Særlige Klageret præsidenten for Højesteret, som skulle føre tilsyn med behandling af oplysninger med hensyn til domstolenes administrative forhold.[759]

---

[757] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 67.

[758] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.8.2. og 4.2.8.3. i de almindelige bemærkninger.

[759] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.8.2. og 4.2.8.3. i de almindelige bemærkninger samt Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 375-379, 416-417 og 518-520.

Udvalgets flertal anså denne ordning for at leve op til kravet om tilsynsmyndighedens fulde uafhængighed.[760]

I Justitsministeriets lovforslag var det imidlertid Domstolsstyrelsen som blev gjort til tilsynsmyndighed for domstolenes administrative funktioner.[761] Dette antages ikke at have ændret på tilsynets uafhængighed.

Domstolsstyrelsen tilsyn omfatter således som nævnt ovenfor efter persondatalovens § 67, stk. 2, kun behandling af oplysninger med hensyn til domstolenes administrative forhold.

Herom fremgår det af bemærkningerne til persondataloven, at Domstolsstyrelsens tilsyn ikke omfatter retternes judicielle funktioner, idet der for disse funktioner er fastsat en særlig kontrolordning.[762]

Den særlige kontrolordning fastsættes i persondatalovens § 67, stk. 3, hvorefter det for *anden behandling end til administrative forhold* er *vedkommende ret*, der træffer afgørelse. Afgørelsen kan kæres til højere ret. For særlige domstole, hvis afgørelser ikke kan indbringes for højere ret, kan den i 1. pkt. nævnte afgørelse kæres til den landsret, i hvis kreds retten er beliggende. Kærefristen er 4 uger fra den dag, afgørelsen er meddelt den pågældende.

Herom fremgår det af bemærkningerne til persondataloven, at der med hensyn til domstolenes *judicielle funktioner* med loven blev gennemført en ordning, hvorefter lovligheden af behandling af oplysninger, der sker i tilknytning til denne virksomhed, gøres til judicielle afgørelser, der træffes af vedkommende dataansvarlige domstol. Endvidere fremgår det, at afgørelserne skal kunne efterprøves ved kære til en højere ret, idet der efter direktivets artikel 28, stk. 1, skal være mulighed for, at den registrerede kan få kontrolleret den dataansvarliges behandling af oplysninger om vedkommende hos en funktionelt uafhængig offentlig myndighed, og der således altid skal være en efterfølgende kontrol af behandlingens lovlighed.[763]

Derudover fremgår det af Registerudvalgets betænkning, at direktivets artikel 28 primært synes at tage sigte på den behandling af oplysninger, som finder sted hos den offentlige

[760] Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 378.
[761] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.8.3. i de almindelige bemærkninger.
[762] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 67.
[763] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.8.2. og 4.2.8.3. i de almindelige bemærkninger.

forvaltning og hos private, og at reglerne i bestemmelsen på baggrund af udformningen heraf ikke på samme måde tager sigte på den behandling af oplysninger, som finder sted hos domstolene, i hvert fald ikke den behandling, som sker i tilknytning til domstolenes udøvelse af *judicielle funktioner.*[764]

På den baggrund kom Registerudvalget frem til, at det næppe kan antages, at der efter direktivet stilles krav om, at en offentlig tilsynsmyndighed af egen drift – eller for den sags skyld efter klage – skal kunne foretage kontrol med den behandling af oplysninger, som foretages i forbindelse med domsskrivningen mv.[765]

En ordning, hvorefter vedkommende tilsynsmyndighed kan beordre oplysninger, som anvendes i forbindelse med domstolenes afgørelse af en sag, slettet, berigtiget eller blokeret, kan næppe antages at være påkrævet efter direktivet. Der lægges herved vægt på, at formålet med artikel 28 er at sikre, at den enkelte medlemsstat gennemfører en ordning, hvorefter der gives en registreret person mulighed for hos en funktionelt uafhængig myndighed at få kontrolleret, om behandlingen af oplysninger om den pågældende er sket i overensstemmelse med lovgivningens regler herom.

Behovet for, at en tilsynsmyndighed af *egen drift* kontrollerer dette, vil navnlig være til stede i de situationer, hvor den registrerede person ikke er klar over, at der sker behandling af oplysninger om vedkommende selv. I de situationer, hvor registrerede personer er bekendt med, at der behandles
oplysninger om dem, gør behovet for, at vedkommende tilsynsmyndighed af egen drift foretager kontrol af behandlingerne, sig derimod ikke gældende på samme måde. I sådanne situationer vil den registrerede nemlig have en viden, der gør vedkommende i stand til at vurdere lovligheden af behandlingen af oplysninger, og dermed også om vedkommende ønsker lovligheden kontrolleret hos den kompetente myndighed.

Det bemærkes i den forbindelse, at personer, som er involveret i en retssag (parter og vidner), vil være bekendt med, at der i forbindelse med retssagens behandling foretages behandling af oplysninger om dem. Der vil derfor ikke være noget større behov for, at en tilsynsmyndighed af egen drift påser overholdelsen af lovgivningen i forbindelse med selve behandlingen af oplysninger i tilknytning til judiciel virksomhed. I lyset af det ovennævnte synes det derfor af principielle grunde rigtigst, at de dataansvarlige domstole ikke i forbindelse med varetagelsen af deres judicielle funktioner, undergives kontrol af vedkommende

[764] Registerudvalget betænkning nr. 1345/1997 om behandling af personoplysninger, s. 377 f.
[765] Registerudvalget betænkning nr. 1345/1997 om behandling af personoplysninger, s. 378.

tilsynsmyndighed. Dette er også bedst stemmende med grundlovens principper om domstolenes uafhængighed.[766]

Registerudvalget synes således ikke at have anset domstolenes judicielle funktioner for omfattet af kravet om uafhængigt tilsyn efter direktivet.

7.2.2.2.3. Forholdet til EU-Domstolens retspraksis om uafhængighedskriteriet

Det bemærkes, at de domme fra EU-Domstolen, som er omtalt ovenfor under forrige afsnit, ikke har givet anledning til at foretage ændringer i den danske tilsynsordning. Bl.a. har Justitsministeriet om forholdet mellem den danske tilsynsordning og dommen i sagen C-614/10 i et svar på et spørgsmål fra Folketingets Retsudvalg[767] anført, at dommen efter ministeriets opfattelse ikke kan antages at rejse spørgsmål i forhold til gennemførelsen af databeskyttelsesdirektivets artikel 28, stk. 1, 2. pkt. i dansk ret. Justitsministeriet fandt i den forbindelse, at Datatilsynets organisatoriske sammenhæng med ministeriet ikke kan sammenlignes med den omstridte østrigske ordning, og at der heller ikke foreligger en grad af integration mellem ministeriet og tilsynet, som medfører, at tilsynet ikke udøver sine funktioner i fuld uafhængighed.

7.2.3. Databeskyttelsesforordningen

7.2.3.1. Indledning

Databeskyttelsesforordningens artikel 51 fastsætter, at der skal oprettes uafhængige tilsynsmyndigheder i medlemsstaterne. I artikel 52 fastsættes, at disse myndigheder skal være fuldt uafhængige og en række specifikke krav, som må anses at skulle sikre tilsynsmyndighedernes fulde uafhængighed.

Det bemærkes, at der endvidere for tilsynsmyndighederne er fastsat specifikke regler i forordningens artikel 53-54 om betingelser for medlemmer af tilsynsmyndighederne og regler om oprettelse af tilsynsmyndighederne, som må anses at skulle være med til at sikre deres fulde uafhængighed.

På baggrund af Kommissionens oprindelige forslag[768] sammenholdt med den vedtagne forordning må det anses at være hensigten, at artikel 52 skal videreføre uafhængighedskravet i det gældende databeskyttelsesdirektivs artikel 28, stk. 1, herunder EU-Domstolens fortolkning af kravet.

---

[766] Registerudvalget betænkning nr. 1345/1997 om behandling af personoplysninger, s. 378.

[767] Justitsministeriets svar af 17. december 2012 på spørgsmål nr. 284 (Alm. del), som Folketingets Retsudvalg har stillet til ministeren den 19. november 2012.

[768] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), afsnit 3.4.6.1 i forslagets begrundelse smh. forslagets artikel 47.

7.2.3.2. Uafhængighedskravet

Det følger af forordningens artikel 52, *stk. 1*, at medlemsstaterne skal sikre, at hver tilsynsmyndighed skal udføre sine opgaver og udøve sine beføjelser i henhold til forordningen i fuld uafhængighed.

På baggrund af at der som nævnt er tale om en videreførelse af EU-Domstolens fortolkning af begrebet "fuld uafhængighed", kan der for en nærmere forståelse heraf henvises til EU-Domstolens retspraksis herom som omtalt ovenfor.

Som nævnt i dette afsnit skal begrebet fortolkes i lyset af formålet med uafhængighedskriteriet, som er at sikre et effektivt og pålideligt tilsyn med overholdelsen af reglerne i forordningen.

Tilsynsmyndighederne skal således være funktionelt uafhængige, og deres beslutninger skal stå uden for enhver mistanke om partiskhed og skal beskyttes imod enhver form for udefrakommende påvirkning, herunder direkte eller indirekte påvirkning.

Det betyder bl.a., at tilsynsmyndighederne ikke må være en integreret del af en almindelig statslig myndighed eller underlagt et almindeligt statsligt tilsyn. Omvendt er der ikke noget til hinder for, at tilsynsmyndighederne underkastes tilsynsmekanismer, hvad angår deres finansielle udgifter eller underkastes almindelig domstolskontrol, jf. forordningens præambelbetragtning nr. 118 og artikel 52, stk. 6. Tilsynsmyndighederne skal heller ikke nødvendigvis have en selvstændig budgetpost for at kunne opfylde uafhængighedskriteriet og kan dermed i budgetmæssig henseende henhøre under et bestemt ministerområde.

7.2.3.2.1. Tilsynsmyndighedernes medlemmer

Efter forordningens artikel 52, *stk. 2*, skal medlemmet eller medlemmerne af hver tilsynsmyndighed i forbindelse med udførelsen af deres opgaver og udøvelsen af deres beføjelser i he nhold til forordningen være frie for direkte eller indirekte udefrakommende indflydelse og må hverken søge eller modtage instrukser fra andre.

Bestemmelsen fastsætter nærmere regler om tilsynsmyndighedernes medlemmers uafhængighed. Bestemmelsen er tæt forbundet med forordningens artikel 53, der fastsætter nærmere krav til udnævnelse af tilsynsmyndighedernes medlemmer, embedsperiodens ophør og afskedigelse, og som er med til at sikre medlemmernes uafhængighed.

Medlemmet eller medlemmerne må antages at udgøre den personale- og beslutningsmæssige ledelse af tilsynsmyndighederne. Det bemærkes, at dette, i en dansk kontekst, må være

Datatilsynets direktør. Efter almindelige forvaltningsretlige principper kan medlemmet delegere sin kompetence til andre, herunder ansatte i tilsynsmyndigheden.

Med anvendelsen af ordvalget *medlemmet eller medlemmerne* lades det være op til medlemsstaterne selv at beslutte, hvor mange medlemmer deres tilsynsmyndighed eller -myndigheder skal bestå af.

Som følge af EU-Domstolens retspraksis må kriteriet om, at medlemmerne skal være frie for indflydelse, bl.a. indebære, at medlemmerne ikke må være under ledelse af en person uden for tilsynsmyndigheden, som kan udøve tjenstlig kontrol med medlemmerne eller på anden måde medføre risiko for, at der øves indflydelse på tilsynsmyndighedens afgørelser.

Efter forordningens artikel 52, *stk. 3*, skal medlemmerne af den enkelte tilsynsmyndighed afholde sig fra enhver handling, der er uforenelig med deres hverv, og må ikke, så længe deres embedsperiode varer, udøve uforenelig lønnet eller ulønnet virksomhed.

De handlinger, som et medlem skal afholde sig fra efter denne bestemmelse, skal ses i sammenhæng med det overordnede krav til myndighedens uafhængighed, som bestemmelsen har til formål af understøtte, og i sammenhæng med artikel 52, stk. 2, om at den pågældende skal være fri for udefrakommende indflydelse.

Det følger af præambelbetragtning nr. 121, at medlemmet eller medlemmerne for at sikre tilsynsmyndighedens uafhængighed bør handle med integritet.

Hertil kan det føjes, at det som nævnt i ovenstående afsnit følger af EU-Domstolens retspraksis, at tilsynsmyndighedernes og dermed medlemmernes beslutninger skal stå uden for enhver mistanke om partiskhed. Medlemmerne – eller i hvert fald det administrerende medlem – må således ifølge bestemmelsen ikke handle på en sådan måde, at der opstår interessekonflikter, så de bliver inhabile, idet der herved i så fald vil kunne opstå mistanke om det pågældende medlems partiskhed og dermed hele tilsynsmyndighedens partiskhed.

En klar rettesnor for, hvornår der bl.a. kan være en interessekonflikt, kan formentlig udledes af grundlæggende habilitetskrav, som f.eks. er fastsat i forvaltningslovens § 3, stk. 1.

Et medlem må efter forordningens artikel 52, stk. 3, således antages så vidt muligt at skulle afholde sig fra handlinger, som gør, at medlemmet kan få en særlig personlig eller økonomisk interesse i udfald af tilsynsmyndighedens sager, og må ikke samtidig med hvervet være repræsentant for nogen, der har en sådan interesse.

7.2.3.2.2. Tilsynsmyndighedernes ressourcer

Ifølge artikel 52, *stk. 4*, skal medlemsstaterne sikre, at den enkelte tilsynsmyndighed råder over de nødvendige menneskelige, tekniske og finansielle ressourcer samt lokaler og infrastruktur til effektivt at kunne udføre sine opgaver og udøve sine beføjelser, herunder opgaver og beføjelser vedrørende gensidig bistand samt samarbejde med og deltagelse i Databeskyttelsesrådet.

Det følger af forordningens præambelbetragtning nr. 120, at hver tilsynsmyndighed bør have de nødvendige finansielle og menneskelige ressourcer samt lokaler og infrastruktur til effektivt at kunne udføre sine opgaver, herunder opgaver vedrørende gensidig bistand og samarbejde med andre tilsynsmyndigheder i hele Unionen.

Ifølge den ovenfor nævnte retspraksis fra EU-Domstolen er det nødvendigt for opfyldelse af uafhængighedskriteriet, at der tildeles de nødvendige ressourcer.

Den nærmere opgørelse af, hvad der er nødvendige ressourcer hænger sammen med tilsynets opgaver og beføjelser, hvortil der skal være de nødvendige menneskelige kompetencer, et tilstrækkeligt antal medarbejdere, IT-infrastruktur, tilstrækkeligt med lokaleplads mv.

7.2.3.2.3. Tilsynsmyndighedernes personale

Ifølge artikel 52, *stk. 5*, skal hver medlemsstat sikre, at den enkelte tilsynsmyndighed vælger og råder over sit eget personale, der alene er under ledelse af medlemmet eller medlemmerne af den pågældende tilsynsmyndighed.

Der sondres således i artikel 52 mellem tilsynsmyndighedernes *medlemmer* og *personale*.

Artikel 52, stk. 5, har sammenhæng med artikel 52, stk. 1, om fuld uafhængighed og artikel 52, stk. 2, om at medlemmerne skal være fri for udefrakommende indflydelse. Hvis personalet hos tilsynsmyndighederne f.eks. ansættes af eller ledes af f.eks. en anden myndighed, ville dette skabe risiko for udefrakommende indflydelse (fra den pågældende anden myndighed) på tilsynsmyndigheden, herunder dens medlemmer.

Tilsynsmyndigheden skal således efter bestemmelsens ordlyd selv vælge sit personale. Det følger imidlertid af forordningens præambelbetragtning nr. 121, at tilsynsmyndigheden skal have sit eget personale, der er udvalgt af tilsynsmyndigheden *eller* et uafhængigt organ, der er oprettet ved medlemsstaternes nationale ret.

7.2.3.2.4. Finansiel kontrol med tilsynsmyndighederne
Ifølge artikel 52, *stk. 6*, skal hver medlemsstat sikre, at den enkelte tilsynsmyndighed er underlagt finansiel kontrol, som ikke påvirker dens uafhængighed, og at den fører særskilte offentlige årsbudgetter, der kan være en del af det samlede statsbudget eller nationale budget.

Det skal således for det første sikres, at tilsynsmyndighederne er underlagt finansiel kontrol.

Af forordningens præambelbetragtning nr. 118 følger det herom, at tilsynsmyndighedernes uafhængighed ikke betyder, at tilsynsmyndighederne ikke kan underkastes kontrol eller tilsynsmekanismer, hvad angår deres finansielle udgifter.

Der skal på den baggrund bl.a. være kontrol med, at tilsynsmyndighederne ikke misbruger deres midler.

Det skal for det andet sikres, at der føres særskilte eller separate offentlige årsbudgetter for tilsynsmyndighederne. Formålet hermed må bl.a. antages at være, at der skal være gennemsigtighed med de midler, som tildeles tilsynsmyndighederne, samtidig med at der sikres et grundlag for at vurdere, om myndigheden tildeles de fornødne ressourcer i medfør af artikel 52, stk. 4.

7.2.4. Overvejelser
7.2.4.1. Forholdet mellem gældende ret og databeskyttelsesforordningen
Bestemmelserne i artikel 52 er overordnet udtryk for en videreførelse af gældende ret, herunder udtryk for en kodificering af EU-Domstolens retspraksis om fortolkningen af uafhængighedskriteriet i databeskyttelsesdirektivets artikel 28, stk. 1.

Den gældende ordning i Danmark efter persondatalovens §§ 55-56 og §§ 67-68 med Datatilsynets og Domstolsstyrelsens tilsyn anses for at leve op til det gældende uafhængighedskrav, hvorfor den gældende danske ordning må antages at kunne videreføres, når forordningen får anvendelse.

Uafhængighedskriteriet i forordningens artikel 52, stk. 1, vil således erstatte persondatalovens § 56.

Det bemærkes i den forbindelse, at domstolenes judicielle funktioner som nævnt ovenfor ikke anses for omfattet af tilsynsforpligtelsen efter det gældende databeskyttelsesdirektiv. På linje hermed fastsættes det i databeskyttelsesforordningens artikel 55, stk. 3, at tilsyns-

myndighederne i henhold til forordningen ikke har kompetence til at føre tilsyn med domstolenes behandlingsaktiviteter, når disse handler i deres egenskab af domstol. Det er således – ligesom efter det gældende databeskyttelsesdirektivs artikel 28, stk. 1 – som nævnt under afsnit 7.1. ikke et krav efter forordningens artikel 51, stk. 1, og 52, stk. 1, at der skal være et uafhængigt tilsyn med domstolenes judicielle funktioner. Der synes imidlertid ikke at være noget til hinder for at opretholde en bestemmelse svarende til persondatalovens § 67, stk. 3, som fastsætter procedurerne for behandling af klager mv. over behandling af personoplysninger.

Databeskyttelsesforordningens artikel 52, stk. 2 og 3, gælder direkte, hvorimod stk. 4-6 forudsætter, at kravene heri sikres af medlemsstaterne.

I en dansk kontekst må stk. 4 om nødvendige ressourcer antages at kunne opfyldes på samme måde som i dag, ved at bevillingen til Datatilsynet og Domstolsstyrelsen fremgår af den årlige finanslov under Justitsministeriet.

På samme måde indebærer stk. 5 om personale heller ikke nødvendigvis lovgivningsmæssige konsekvenser for Datatilsynet og Domstolsstyrelsen, idet dette ikke hviler på et direkte lovgivningsmæssigt grundlag efter dansk ret. Dog forudsættes tilsynsmyndighederne at indrette sig på kravene i forbindelse med den faktiske udvælgelse af personalet mv.

Stk. 6 om finansiel kontrol synes heller ikke at indebære ændringer i den gældende fremgangsmåde med årlige bevillinger til Datatilsynet og Domstolsstyrelsen på finansloven.

7.2.4.2. Overvejelser om den fremtidige konstruktion for tilsynet i Danmark.

7.2.4.2.1. I forbindelse med overgangen til databeskyttelsesforordningen og de ændringer i lovgivningen, som forordningen indebærer, er det nærliggende at overveje, om den tilsynsordning med delt tilsyn mellem Datatilsynet og Domstolsstyrelsen, som vi kender det i dag, bør bestå, som den er, eller om det er mest hensigtsmæssigt med en ændret ordning.

Efter forordningens artikel 51, stk. 1, kan medlemsstaterne oprette én eller flere uafhængige tilsynsmyndigheder.

Det følger bl.a. af forordningens præambelbetragtning nr. 117, at medlemsstaterne bør kunne oprette mere end én tilsynsmyndighed for at afspejle deres forfatningsmæssige, organisatoriske og administrative struktur. Efter denne præambelbetragtning skal denne mulighed således tilgodese forskellene i medlemsstaternes forfatningsmæssige, organisatoriske og administrative struktur.

Herudover skal samtlige tilsynsmyndigheder omfattet af artikel 51, stk. 1, opfylde uafhængighedskriteriet, jf. artikel 52, stk. 1, og de øvrige krav til tilsynsmyndighederne i forordningen.

I Danmark kan der således opretholdes en tilsynsordning, hvor Datatilsynet er det primære tilsyn, og hvor Domstolsstyrelsen fører tilsynet med domstolenes behandling af personoplysninger med hensyn til administrative forhold. Herudover vil det ikke være udelukket at oprette andre tilsynsmyndigheder, hvor vægtige grunde inden for den danske organisatoriske og administrative struktur. Det vil således bl.a. ikke være udelukket at lade en anden uafhængig myndighed end Datatilsynet føre tilsyn med en specifik sektor.

7.2.4.2.2. Det er endvidere nærliggende at overveje, hvordan de to tilsynsmyndigheder mest hensigtsmæssigt organiseres under iagttagelse af uafhængighedskriteriet mv.

For Datatilsynets vedkommende vil der f.eks. kunne træffes et valg med hensyn til, om tilsynet fortsat skal bestå af både en direktør og et råd. Som anført i afsnit 7.1.3.2.1. kan tilsynsmyndigheden bestå af såvel en som flere medlemmer. Det vil således være tilstrækkeligt, hvis Datatilsynet ledes af en direktør, som er uafhængig i overensstemmelse med artikel 52, stk. 2, og udnævnes i overensstemmelse med reglerne i forordningens artikel 53.

Det samme gør sig i princippet gældende i forhold til Domstolsstyrelsen. Dog varetager Domstolsstyrelsen også en række andre funktioner, som har en betydelig indflydelse på, hvordan styrelsen organiseres. Domstolsstyrelsens overordnede ledelse er en bestyrelse bestående af en højesteretsdommer, to landsdommere, to byretsdommere, en repræsentant for det øvrige akademiske personale ved domstolene, to repræsentanter for det administrative personale ved domstolene, en advokat og to medlemmer med særlig ledelsesmæssig og samfundsmæssig indsigt. Sammensætningen af bestyrelsen som en form for kollegialt organ må anses for at sikre den fornødne uafhængighed.

Beskyttelsen af personoplysninger er i dag omfattet af regler i flere forskellige love (bl.a. persondataloven, lov om finansiel virksomhed og lov om betalingstjenester og elektroniske penge) og under tilsyn af flere myndigheder (bl.a. Datatilsynet, Domstolsstyrelsen, Finanstilsynet og Forbrugerombudsmanden). Dog er det alene Datatilsynet og Domstolsstyrelsen, der har status som uafhængige tilsynsmyndigheder i det gældende databeskyttelsesdirektivs og fremadrettet i databeskyttelsesforordningens forstand.

Der er i forbindelse med kortlægningen af beskyttelse af oplysninger om borgernes elektroniske betalinger som følge af den såkaldte Se og Hør-sag[769] blevet peget på, at der mangler en klar afgrænsning mellem disse forskellige tilsynsførende myndigheders kompetencer, og at der mangler et formaliseret samarbejde mellem myndighederne.

En sådan klar afgrænsning kunne komme i forbindelse med vedtagelsen af en ny persondatalov. Der vil i den forbindelse skulle tages stilling til, i hvilket omfang det er relevant og hensigtsmæssigt at have mere end en tilsynsmyndighed i forordningens forstand. Videreføres den gældende tilsynsordning i Danmark, således at Datatilsynet – ligesom med persondataloven – fører det generelle tilsyn med overholdelsen af forordningens regler, vil forordningen indebære, at Datatilsynet har tilsynskompetence på alle områder inden for dansk jurisdiktion omfattet af forordningens anvendelsesområde, herunder områder undergivet dansk særregulering fastsat i overensstemmelse med forordningen. Det gælder dog ikke behandling af oplysninger for domstolene, som er undergivet Domstolsstyrelsens tilsynskompetence. De øvrige tilsyn, såsom Finanstilsynet og Forbrugerombudsmanden, der ikke har status som uafhængige tilsynsmyndigheder, vil alene have karakter af *supplerende* tilsyn i forhold til Datatilsynets generelle tilsyn.

7.3. Regler om oprettelse af en tilsynsmyndighed, artikel 54

7.3.1. Præsentation

I databeskyttelsesforordningens artikel 51, stk. 1 og 3, artikel 52, stk. 2-4, artikel 53, stk. 1, og artikel 54, stk. 1, er fastsat bestemmelser om tilsyn, som skal gennemføres i medlemsstaternes nationale ret.

Særligt forordningens artikel 54, stk. 1, indeholder specifikke krav til, at medlemsstaterne ved eller i henhold til lov fastsætter regler om oprettelse af tilsynsmyndigheder og krav til tilsynsmyndighedernes medlemmer og personale. Bestemmelsen skal bl.a. sammenholdes med forordningens artikel 51-53 med henblik på den nærmere fastlæggelse af kravene til medlemsstaternes lovgivning.

7.3.2. Regler om oprettelse af tilsynsmyndigheder

Efter databeskyttelsesforordningens artikel 54, stk. 1, *litra a*, sammenholdt med artikel 51, stk. 1, er Danmark forpligtet til at oprette mindst én uafhængig tilsynsmyndighed ved lov eller bekendtgørelse i henhold til lov.

[769] Rapport af juni 2016 om kortlægning af beskyttelsen af oplysninger om borgernes elektroniske betalinger mv., afgivet af en arbejdsgruppe under Justitsministeriet, s. 89.

Hvis der ønskes flere tilsynsmyndigheder, skal de øvrige også ifølge bestemmelsen oprettes ved lov eller i henhold til lov. Endvidere skal der i givet fald ifølge artikel 51, stk. 3, udpeges én tilsynsmyndighed, der repræsentere disse myndigheder i Databeskyttelsesrådet, og fastsættes en mekanisme, som sikrer, at de andre myndigheder overholder reglerne vedrørende den sammenhængsmekanisme, der er omhandlet i artikel 63. Udpegelse af en koordinerende tilsynsmyndighed antages ikke at skulle ske ved eller i henhold til lov.

Den omstændighed, at tilsynsmyndighederne skal være fuldt uafhængige, jf. herved artikel 51, stk. 1, og artikel 52, stk. 1, stiller nærmere krav til oprettelsen ved eller i henhold til lov, f.eks. at de ikke må være underlagt regeringen eller som udgangspunkt ikke må være underlagt et andet (statsligt) tilsyn eller instruks fra en anden myndighed.

7.3.3. Regler om tilsynsmyndighedernes medlemmer og personale

7.3.3.1. Regler og procedurer for udnævnelse af medlemmer

Som led i kravet om tilsynsmyndighedernes fulde uafhængighed er der efter forordningens artikel 52, stk. 2-3, præciseret en række krav til medlemmerne af tilsynsmyndighederne.

Kravet i artikel 52, stk. 2, om medlemmernes uafhængighed suppleres af forordningens artikel 53, stk. 1, hvorefter medlemsstaterne skal sikre, at hvert medlem af en tilsynsmyndighed udnævnes efter en gennemsigtig procedure af deres parlament, regering, statschef eller et uafhængigt organ.

I forordningens artikel 54, stk. 1, *litra c*, er det præciseret, at reglerne og procedurerne for udnævnelse af medlemmer skal fastsættes ved eller i henhold til lov.

Danmark er således efter forordningen forpligtet til ved lov eller bekendtgørelse at fastsætte regler og procedurer for udnævnelse af medlemmer af tilsynsmyndighederne. Det må antages, at det herved skal sikres, at proceduren er gennemsigtig, og at udnævnelsen sker på det niveau eller af et uafhængigt organ som foreskrevet i artikel 53, stk. 1.

7.3.3.2. Regler om medlemmers embedsperiode

Reglerne i forordningens artikel 52, stk. 2-3, suppleres endvidere af forordningens artikel 53, stk. 3, der fastsætter nærmere regler om ophør af medlemmernes embedsperiode.

Efter forordningens artikel 54, stk. 1, *litra d – litra e*, er Danmark forpligtet til ved lov eller bekendtgørelse at fastsætte regler om embedsperioden for og mulighed for genudnævnelse af medlemmer, der som altovervejende udgangspunkt varer i mindst fire år.

7.3.3.3. Regler om medlemmernes kvalifikationer
Af forordningens artikel 53, stk. 2, følger der nærmere krav til medlemmernes kvalifikationer mv.

I forordningens artikel 54, stk. 1, *litra b*, følger det, at det skal fastsættes ved eller i henhold til lov, hvad de nødvendige kvalifikationer og udvælgelseskriterier for medlemmer er.

Ved fastlæggelsen af, hvad der er nødvendige kvalifikationer og udvælgelseskriterier, efterlades et vist skøn, der dog er bundet af kriterierne i artikel 53, stk. 2, om at medlemmer skal have de kvalifikationer, den erfaring og kompetence på databeskyttelsesområdet, der er nødvendig for at varetage hvervet og udøvelse af de beføjelser, som medlemmer skal. Dette skal sammenholdes med tilsynsmyndighedernes kompetencer, opgaver og beføjelser, som er fastlagt i forordningens kapitel VI, 2. afdeling.

7.3.3.4. Regler om krav til medlemmers og personalets adfærd
Af forordningens artikel 52, stk. 3, stilles der nærmere krav til medlemmernes adfærd, nærmere bestemt hvilke handlinger de skal afholde sig fra. Supplerende til denne bestemmelse følger der bestemmelser af forordningens artikel 53, stk. 4, om hvornår medlemmer må afskediges. I forordningens artikel 54, stk. 1, *litra f*, er der fastsat et specifikt krav om, at medlemsstaterne ved lov eller i henhold til lov fastsætter betingelserne for medlemmerne og personalet, forbud mod handlinger, hverv og fordele, der er uforenelige hermed, under og efter embedsperioden, og regler for arbejdsophør.

Der er herved også overladt medlemsstaterne et vist skøn med hensyn til, hvilke handlinger mv., der er uforenelige med hvervet som medlem og personale.

7.3.4. Øvrige krav
I forordningens artikel 52, stk. 4-6, er der krav om, at medlemsstaterne skal sikre, at tilsynsmyndighederne har de nødvendige ressourcer mv., vælger og råder over eget personale samt er underlagt finansiel kontrol, som ikke påvirker deres uafhængighed.

Reglerne anses ikke umiddelbart at forudsætte fastsættelse af nationale regler ved lov eller i henhold til lov. Dog må det i en dansk kontekst for så vidt angår bestemmelsen om finansiel kontrol anses at indebære, at tilsynsmyndighedernes budgetter fremgår af finansloven.

Endelig er der efter forordningens artikel 54, stk. 2, et krav om, at tilsynsmyndighedernes medlemmer og personale er undergivet tavshedspligt i overensstemmelse med bl.a. medlemsstaternes nationale ret. Det nærmere indhold af de nationale tavshedspligtsregler, herunder sanktioner i forbindelse med overtrædelse, må anses for at være overladt til med-

lemsstaterne. Af hensyn til EU-rettens effektive virkning må det herved anses at være et krav, at tavshedspligtsreglerne ikke er lempeligere end andre sammenlignelige tavshedspligtsregler, som gælder i medlemsstaterne.

7.4. Tilsynsmyndighedens kompetence, artikel 55 og 56

7.4.1. Præsentation

Databeskyttelsesforordningens artikel 55, stk. 1, fastslår, at det er den nationale tilsynsmyndighed, som er kompetent til at udøve opgaver og beføjelser inden for dens egen medlemsstats område.

Forordningens bestemmelser om den såkaldte one-stop-shop mekanisme, som er en konsekvens af forordningens artikel 56, der henviser til artikel 60 og kapitel VII, indebærer imidlertid, at der i visse tilfælde er en ledende tilsynsmyndighed, som er kompetent til at agere i en konkret sag. I disse tilfælde er den nationale tilsynsmyndighed som udgangspunkt ikke kompetent til at handle på egen hånd.

7.4.2. Gældende ret

Datatilsynet har som udgangspunkt kompetence over for enhver behandling, der omfattes af loven, jf. herved persondatalovens § 55 og reglerne i lovens kapitel 1 om lovens område (§§ 1 og 2) samt kapitel 3 om lovens geografiske område (§ 4). Tilsyn med behandling af personoplysninger, der foretages for domstolene, føres dog af Domstolsstyrelsen og de overordnede retter, jf. reglerne i kapitel 17.

Databeskyttelsesdirektivet indeholder i artikel 4 en bestemmelse om det geografiske gyldighedsområde for den nationale lovgivning, som gennemfører direktivet. Bestemmelsen, der er gennemført i dansk ret ved persondatalovens § 4, har ifølge Registerudvalgets betænkning nr. 1345 karakter af en lovvalgsregel.[770] Det fremgår endvidere af betænkningen dette sted, at bestemmelsen må antages at være tiltænkt samme fællesskabsretlige betydning i de enkelte medlemsstater. Der henvises herved til, at formålet med bestemmelsen dels er at undgå, at personer unddrages beskyttelse ved omgåelse af lovgivningen, dels er at undgå kumulativ anvendelse af flere forskellige lovgivninger, jf. bl.a. direktivets præambelbetragtning 18.

Efter persondatalovens § 4, stk. 1, gælder lovens regler for behandling af personoplysninger, som udføres for en dataansvarlig, der er etableret i Danmark, hvis aktiviteterne finder sted inden for Det Europæiske Fællesskabs område. Et dansk datterselskab af en virksom-

[770] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 218.

hed i et tredjeland skal således leve op til persondataloven, for så vidt angår de personoplysninger, som datterselskabet er ansvarlig for. Uden for bestemmelsen falder de tilfælde, hvor en dataansvarlig, som er etableret uden for dansk område, f.eks. i en anden medlemsstat, udøver aktiviteter på dansk område.

Oplysninger, der opbevares på dansk område for en dataansvarlig, som er etableret i en anden medlemsstat, er således som udgangspunkt ikke omfattet af lovens regler. Dog gælder lovens sikkerhedsregler for behandlinger, som foretages af databehandlere i Danmark, uanset behandlingen i øvrigt er undergivet en anden medlemsstats lovgivning, jf. lovens § 41, stk. 3, 2. pkt. Endvidere gælder lovens regler om Datatilsynets jurisdiktionskompetence i relation til sådanne behandlinger, jf. lovens § 64, stk. 1. Tilsynets kompetence udøves i så fald på baggrund af fremmed ret.

Denne sidstnævnte bestemmelse, persondatalovens § 64, bygger på databeskyttelsesdirektivets artikel 28, stk. 6, hvorefter den enkelte tilsynsmyndighed – uanset hvilken national lov der måtte gælde for den pågældende behandling – er kompetent til på sin medlemsstats område at udøve de beføjelser, der tillægges den i overensstemmelse med artikel 28, stk. 3. Myndigheden kan blive anmodet om at udøve sine beføjelser af en myndighed i en anden medlemsstat. Endvidere fremgår det, at tilsynsmyndighederne samarbejder med hinanden i det omfang, det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle nyttige oplysninger.

Efter § 64, stk. 1, kan Datatilsynet af egen drift eller efter anmodning fra en anden medlemsstat påse, at en behandling af oplysninger, som finder sted i Danmark, er lovlig, uanset at den pågældende behandling er undergivet en anden medlemsstats lovgivning. Bestemmelserne i §§ 59 og 62 finder tilsvarende anvendelse.

Datatilsynet er således med andre ord kompetent til at påse, at en behandling, som er undergivet en anden medlemsstats lovgivning er lovlig. Datatilsynet vil kunne kræve oplysninger af en eventuel databehandler, som er etableret i Danmark, eller af en repræsentant for den dataansvarlige, som befinder sig i Danmark, jf. § 62, stk. 1. Tilsynet vil endvidere kunne udføre tilsyn efter reglerne i § 62, stk. 3-4. Herudover har tilsynet kompetence til at realitetsbehandle og afgøre sagen efter den pågældende medlemsstats materielle lovgivning. Dette må forventes at ske på grundlag af oplysninger fra tilsynsmyndigheden i det pågældende medlemsland. Endelig kan Datatilsynet efter § 59 meddele påbud eller forbud til en databehandler eller en repræsentant for den dataansvarlige, hvis disse befinder sig i Danmark. Der er ikke en egentlig klageadgang for de registrerede, men tilsynet er – som det fremgår af ordlyden – kompetent til at tage en sag op af egen drift, hvis tilsynet finder

anledning dertil, ligesom en myndighed i en anden medlemsstat kan anmode Datatilsynet om at udøve sine beføjelser.

Det fremgår endvidere af lovens § 64, stk. 2, at Datatilsynet kan videregive oplysninger til tilsynsmyndigheder i andre medlemsstater i det omfang, det er nødvendigt for at påse overholdelsen af bestemmelserne i denne lov eller af den pågældende medlemsstats databeskyttelseslovgivning.

7.4.3. Databeskyttelsesforordningen

7.4.3.1. Databeskyttelsesforordningens artikel 55, stk. 1 - generel kompetence

Det fremgår af forordningens artikel 55, stk. 1, at hver tilsynsmyndighed er kompetent til at udføre de opgaver og udøve de beføjelser, der tillægges den i overensstemmelse med denne forordning, på sin egen medlemsstats område.

Artikel 55, stk. 1, fastslår således, at det er den nationale tilsynsmyndighed, som er kompetent til at udøve opgaver og beføjelser inden for dens egen medlemsstats område, jf. dog artikel 56 nedenfor.

Vedrørende forordningens kompetenceregler fremgår endvidere af præambelbetragtning nr. 122**,** at hver tilsynsmyndighed på sin egen medlemsstats område bør have kompetence til at udøve sine beføjelser og varetage de opgaver, der er tildelt den i henhold til denne forordning. Dette bør navnlig omfatte behandling, som foretages som led i aktiviteter, der udføres for den dataansvarliges eller databehandlerens etablering på dens egen medlemsstats område, behandling af personoplysninger, der udføres af offentlige myndigheder eller af private organer i offentlighedens interesse, behandling, der påvirker registrerede på dens område, eller behandling, der udføres af en dataansvarlig eller en databehandler, som ikke er etableret i Unionen, når den er rettet mod registrerede, som har bopæl på dens område. Dette bør omfatte behandling af klager, der er indgivet af en registreret, udførelse af undersøgelser vedrørende denne forordnings anvendelse og en indsats for at fremme offentlighedens bevidstgørelse om risici, regler, garantier og rettigheder i forbindelse med behandling af personoplysninger.

7.4.3.2. Databeskyttelsesforordningens artikel 55, stk. 2 - enekomptence

Af forordningens artikel 55, stk. 2, følger, at hvis behandlingen af personoplysninger foretages af offentlige myndigheder eller af private organer, der handler på grundlag af artikel 6, stk. 1, litra c eller litra e, er tilsynsmyndigheden i den pågældende medlemsstat kompetent. I så fald finder artikel 56 ikke anvendelse. Tilsynsmyndigheden er med andre ord i sådanne tilfælde enekompetent.

Om denne situation fremgår det endvidere af præambelbetragtning nr. 128, at reglerne om den ledende tilsynsmyndighed og one-stop-shop mekanismen ikke bør gælde, når behandling foretages af offentlige myndigheder eller af private organer i offentlighedens interesse. I sådanne tilfælde bør kun tilsynsmyndigheden i den medlemsstat, hvor den offentlige myndighed eller det private organ er etableret, have kompetence til at udøve de beføjelser, som den er tillagt i henhold til denne forordning.

7.4.3.3. Databeskyttelsesforordningens artikel 55, stk. 3 – tilsyn med domstolene
I forordningens artikel 55, stk. 3, fastslås det, at tilsynsmyndighederne ikke er kompetente til at føre tilsyn med domstoles behandlingsaktiviteter, når disse handler i deres egenskab af domstol.

7.4.3.4. Databeskyttelsesforordningens artikel 56, stk. 1 – ledende tilsynsmyndighed
Det følger af forordningens artikel 56, stk. 1, at det – uden at det berører artikel 55 – er tilsynsmyndigheden ved den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering, som skal være kompetent til at fungere som ledende tilsynsmyndighed i tilfælde af grænseoverskridende behandling af personoplysninger, der foretages af denne dataansvarlige eller databehandler efter proceduren i artikel 60.

For så vidt angår begreberne ”hovedvirksomhed” og ”grænseoverskridende behandling” er disse nærmere defineret i forordningens artikel 4, nr. 16 og 23.

7.4.3.5. Databeskyttelsesforordningens artikel 56, stk. 2-5 – en undtagelse til hovedreglen
Som en undtagelse hertil fremgår det af forordningens artikel 56, stk. 2, at hver tilsynsmyndighed er kompetent til at behandle en indgivet klage eller en eventuel overtrædelse af forordningens bestemmelser, hvis sagens genstand alene vedrører en etablering i den pågældende medlemsstat, eller alene i væsentlig grad påvirker registrerede i den pågældende medlemsstat.

I de tilfælde, som er nævnt i stk. 2, skal tilsynsmyndigheden straks underrette den ledende tilsynsmyndighed om dette forhold. Herefter – inden for en frist på tre uger efter at være blevet underrettet – skal den ledende tilsynsmyndighed beslutte, om den vil behandle sagen efter proceduren i artikel 60 under hensyntagen til, om der er en dataansvarlig eller databehandler etableret i den medlemsstat, hvor den tilsynsmyndighed, som har informeret ledende tilsynsmyndighed, er beliggende, jf. forordningens artikel 56, stk. 3.

Det fremgår endvidere af forordningens artikel 56, stk. 4, at hvis den ledende tilsynsmyndighed beslutter at behandle sagen, skal proceduren i artikel 60 følges. Tilsynsmyndigheden, som har informeret den ledende tilsynsmyndighed, kan forelægge sidstnævnte et ud-

kast til afgørelse i sagen. Den ledende tilsynsmyndighed skal i givet fald tage størst mulig hensyn til dette udkast, når den udarbejder det udkast til afgørelse, som der er henvist til i artikel 60, stk. 3.

Beslutter den ledende tilsynsmyndighed ikke at behandle sagen, skal den tilsynsmyndighed, som forelagde sagen for den ledende tilsynsmyndighed, ifølge forordningens artikel 56, stk. 5, behandle sagen i overensstemmelse med artikel 61 og 62.

7.4.3.6. Databeskyttelsesforordningens artikel 56, stk. 6 - kontaktpunkt
Efter forordningens artikel 56, stk. 6, skal den ledende tilsynsmyndighed være den dataansvarliges eller databehandlerens eneste kontakt i forbindelse med den grænseoverskridende behandling, der foretages af denne dataansvarlige eller databehandler.

7.4.4. Overvejelser
Med forordningens artikel 55 må udgangspunktet anses som værende det sammen som efter gældende ret, nemlig, at det er den nationale tilsynsmyndighed, som er kompetent til at udøve opgaver og beføjelser inden for dens egen medlemsstats område.

Den væsentligste nyskabelse i forhold til de gældende regler om tilsynsmyndighedernes kompetence er således forordningens artikel 56, der skal ses i sammenhæng med de særlige regler om den såkaldte "one-stop-shop mekanisme", der findes i forordningens kapitel VII, og som indebærer, at én tilsynsmyndighed (den ledende tilsynsmyndighed) i visse grænseoverskridende sager vil være enekompetent til at træffe afgørelse i konkrete sager.

7.5. Tilsynsmyndighedens opgaver, artikel 57

7.5.1. Præsentation
Efter databeskyttelsesforordningens artikel 57 tillægges tilsynsmyndigheden en række opgaver, som skal udøves på tilsynsmyndighedens eget territorium. Selv om opregningen er ganske lang, er den ikke udtømmende, jf. ordene "uden at dette berører andre opgaver, der er fastsat i denne forordning". Det fremgår i den forbindelse også af artikel 57, stk. 1, litra v, at tilsynsmyndigheden skal udføre enhver anden opgave i forbindelse med beskyttelse af personoplysninger.

7.5.2. Gældende ret
7.5.2.1. Opgaver efter databeskyttelsesdirektivet
Tilsynsmyndighedernes opgaver er ikke udførligt beskrevet i databeskyttelsesdirektivet. Af direktivets artikel 28, stk. 1, fremgår det således blot, at hver medlemsstat drager omsorg

for, at der udpeges en eller flere offentlige tilsynsmyndigheder, der har til opgave på dens område at påse overholdelsen af de bestemmelser, medlemsstaten vedtager til gennemførelse af direktivet.

Det fremgår endvidere af direktivets artikel 28, stk. 2, at hver medlemsstat drager omsorg for, at tilsynsmyndighederne høres ved udarbejdelsen af administrative foranstaltninger eller retsforskrifter om beskyttelse af personers rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger.

Herudover fremgår det af direktivets artikel 28, stk. 4, 1. afsnit, at enhver, eventuelt repræsenteret ved en sammenslutning, til tilsynsmyndigheden kan indgive en anmodning om beskyttelse af sine rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger. Den pågældende underrettes om, hvorledes sagen følges op.

7.5.2.2. Opgaver efter persondataloven

Datatilsynets almindelige kompetence til at træffe afgørelse over for private – og i visse tilfælde offentlige – dataansvarlige om iagttagelse af reglerne i loven følger af persondatalovens § 55, stk. 1, hvorefter tilsynet, der består af et råd og et sekretariat, fører tilsyn med enhver behandling, der omfattes af loven. Bestemmelsen har bl.a. sin baggrund i databeskyttelsesdirektivets artikel 28, stk. 1.

Persondatalovens § 55, stk. 1, skal i øvrigt sammenholdes med lovens § 58, stk. 1, hvorefter Datatilsynet af egen drift eller efter klage fra en registreret påser, at behandlingen finder sted i overensstemmelse med loven og regler udstedt i medfør heraf. Enhver registreret person eller virksomhed mv., som er beskyttet af persondataloven, jf. lovens § 1, kan således i overensstemmelse med de almindelige forvaltningsretlige regler indgive en anmodning til Datatilsynet om beskyttelse af sine rettigheder efter loven. Herudover kan Datatilsynet tage sager op af egen drift.

Tredjemand har derimod som udgangspunkt ikke en ret til at klage til Datatilsynet med den følge, at tilsynet skal behandle sagen, men tilsynet kan i sådanne tilfælde tage sagen op af egen drift, hvis der vurderes at være anledning dertil. Persondatalovens § 58, stk. 1, har sin baggrund i artikel 28, stk. 1 og 4.

Når det gælder den offentlige forvaltning, har Datatilsynet efter persondatalovens § 60, stk. 1, kun afgørelseskompetence med bindende virkning over for andre myndigheder i relation til de bestemmelser, som specifikt er nævnt i bestemmelsen. I andre situationer har tilsynet alene kompetence til at afgive uforbindende udtalelser, jf. § 60, stk. 2.

Endvidere gælder i forhold til den offentlige forvaltning persondatalovens § 47, hvorefter Datatilsynet i de tilfælde, hvor tilsynet ikke kan tiltræde udførelsen af en behandling, som foretages for henholdsvis en underordnet myndighed (stk. 1) og en regional eller kommunal myndighed (stk. 2), kan forelægge sagen for henholdsvis vedkommende minister og indenrigs- og sundhedsministeren (nu økonomi- og indenrigsministeren). Forelæggelsen i tilfælde af uenighed kan foretages af såvel myndigheden som Datatilsynet, og proceduren vil kunne anvendes i hvilken som helst situation, hvor der er uenighed om udførelsen af en behandling, uanset om behandlingen skal forelægges Datatilsynet eller ej, jf. nærmere nedenfor.

Bestemmelsen i § 47 finder dog naturligvis ikke anvendelse i de situationer, hvor Datatilsynet i medfør af § 60, stk. 1, træffer bindende afgørelser over for vedkommende myndighed. Persondatalovens § 47, stk. 1, vil i øvrigt ikke være til hinder for, at vedkommende minister inddrages i de tilfælde, hvor en statslig myndighed ikke står i et underordnelsesforhold til den pågældende minister. I en sådan situation har den pågældende minister ikke afgørelseskompetence efter § 47 og vil kun kunne afgøre tvisten med bindende virkning, hvis dette følger af andet retsgrundlag.[771]

Af persondatalovens § 57 fremgår endvidere, 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.

Bestemmelsen, der har sin baggrund i databeskyttelsesdirektivets artikel 28, stk. 2, nævner ikke en pligt til at høre Datatilsynet i forbindelse med udarbejdelse af lovforslag eller i forbindelse med deltagelsen i udarbejdelse af EU-retsakter, konventioner mv. En sådan pligt antages heller ikke at følge af direktivet. Det er imidlertid efter bemærkningerne til persondataloven en forudsætning, at der sker høring af Datatilsynet i forbindelse med udfærdigelse af lovforslag, som fremsættes af regeringen.[772] Endvidere forudsættes det, at vedkommende ressortministerium i forbindelse med sin stillingtagen til et privat lovforslag hører Datatilsynet. På den baggrund bør der – selvom der ikke direkte er peget på det i lovens forarbejder – også ske høring af Datatilsynet over forslag til EU-retsakter, konventioner mv., hvilket også sker i praksis.

[771] Persondataloven med kommentarer (2015), s. 588.
[772] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 57.

Høringspligten i § 57 må antages kun at omfatte retligt bindende retsakter. Udenfor falder dermed bl.a. myndighedernes dispositioner af privatretlig karakter.[773]

Et særligt spørgsmål er, om myndigheders vejledninger er omfattet af persondatalovens § 57. Da en vejledning typisk ikke er bindende, men alene indeholder vejledende retningslinjer for administrationen af det pågældende sagsområde, må udgangspunktet være, at de ikke er omfattet, jf. i den forbindelse også Registerudvalgets betænkning nr. 1345, side 369. I persondataloven med kommentarer, side 624, diskuteres dette imidlertid. Forfatterne bag bogen anfører således, at udstedelse af vejledninger er et hyppigt anvendt og i praksis meget vigtigt styringsmiddel inden for bestemte sagsområder, f.eks. på det sociale område i forhold til kommunerne. Hvis en sådan vejledning rummer vigtige aspekter i forhold til reglerne om behandling af personoplysninger, bør § 57 under alle omstændigheder iagttages.

Det er endvidere forudsat i de almindelige bemærkninger til persondataloven, at Datatilsynet i første række bør tage sigte på at kunne udøve sin virksomhed gennem generelle retningslinjer og ved en serviceorienteret rådgivning og vejledning.[774] Dette sikres bl.a. gennem tilsynets hjemmeside, hvor tilsynet offentliggør relevant praksis. Datatilsynet har endvidere udarbejdet informationspjecer og -tekster samt forskellige vejledninger om persondataloven. Tilsynet deltager tillige løbende med oplæg på konferencer, i undervisningsforløb og afholder møder med myndigheder, virksomheder, organisationer mv.

Som nævnt ovenfor består Datatilsynets arbejde først og fremmest i at administrere persondataloven. Der findes imidlertid i andre love talrige regler, der vedrører behandling af personoplysninger, og som regulerer forhold, der er omfattet af databeskyttelsesdirektivet. Det kan f.eks. være regler, der foreskriver, at behandling af personoplysninger kan eller skal finde sted under bestemte betingelser. Datatilsynet er derfor i praksis derfor ofte nødt til at tage stilling til rækkevidden og betydningen af sådanne regler i lovgivningen for derved at kunne afgøre, om en behandling af personoplysninger, i forhold til persondataloven, kan finde sted og under hvilke betingelser. Hvis Datatilsynet er i tvivl, vil der kunne indhentes en udtalelse fra den relevante myndighed, f.eks. ressortministeriet, om forståelsen af reglerne i den pågældende lov.[775]

Datatilsynet har også opgaver i henhold til enkelte særlove. Det drejer sig bl.a. om følgende love: Lov om massemediers informationsdatabaser (§ 3 og § 6), lov om værdipapirhan-

[773] Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, s. 369.
[774] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.8.3. i de almindelige bemærkninger.
[775] Persondataloven med kommentarer (2015), s. 618.

del mv. (§ 91), arkivloven (§ 9, § 21, stk. 2, § 23, stk. 2, § 34, § 41, stk. 1, og § 46, stk. 2), lov om Danmark tiltrædelse af Schengen-konventionen (§ 2, stk. 3), lov om Danmarks tiltrædelse af konventionen om gensidig bistand og samarbejde mellem toldmyndighederne (Napoli II-konventionen, § 4, stk. 2), udlændingelovens § 58 c, stk. 3 (vedrørende Dublin-forordningen), og § 58 i, stk. 6 (vedrørende Eurodac-forordningen), og lov om betalingstjenester og elektroniske penge (§ 86, stk. 4).[776]

Datatilsynet deltager i internationalt samarbejde på databeskyttelsesområdet. Tilsynet deltager bl.a. i:

- i den arbejdsgruppe, der er nedsat i henhold til artikel 29 i databeskyttelsesdirektivet (Artikel 29-gruppen).
- koordinationsgrupper for tilsyn med Schengen-informationssys-temet (SIS II SCG), Told-informationssystemet (CIS SCG), Eurodac (ESCG), Visum-informationssystemet (VIS SCG) og Informationssystemet for det Indre Marked (IMI SCG)

De hidtil gældende registerlove er fortsat gældende i begrænset omfang for Færøerne. Datatilsynet varetager de opgaver, der på disse områder er tillagt Registertilsynet i henhold til registerlovene. For så vidt angår Grønland er persondataloven den 1. december 2016 sat i kraft i Grønland med de afvigelser, som de særlige grønlandske forhold tilsiger, jf. anordning nr. 1238 af 15. oktober 2016.

7.5.3. Databeskyttelsesforordningen

7.5.3.1. Tilsynsmyndighedens opgaver (artikel 57, stk. 1, litra a-v)

7.5.3.1.1. Databeskyttelsesforordningens artikel 57, stk. 1, litra a

Af forordningens artikel 57, stk. 1, litra a, fremgår det, at hver tilsynsmyndighed på sit område skal føre tilsyn med og håndhæve anvendelsen af forordningen.

Formelt set svarer denne opgave til den opgave, Datatilsynet har i dag efter persondatalovens § 55, jf. § 60, med at føre tilsyn med behandlinger omfattet af persondataloven.

7.5.3.1.2. Databeskyttelsesforordningens artikel 57, stk. 1, litra b, litra d og litra e

Hver tilsynsmyndighed skal ifølge forordningens artikel 57, stk. 1, litra b, fremme offentlighedens kendskab til og forståelse af risici, regler, garantier og rettigheder i forbindelse med behandling, og der skal sættes særlig fokus på aktiviteter, der er direkte rettet mod børn.

[776] Persondataloven med kommentarer (2015), s. 618.

Tilsynsmyndigheden skal endvidere ifølge forordningens artikel 57, stk. 1, litra d, fremme dataansvarliges og databehandleres kendskab til deres forpligtelser i henhold til denne forordning.

Herudover følger det af forordningens artikel 57, stk. 1, litra e, at hver tilsynsmyndighed efter anmodning informerer registrerede om udøvelse af deres rettigheder i henhold til denne forordning og med henblik herpå samarbejder med tilsynsmyndighederne i andre medlemsstater, hvis det er relevant.

Som det fremgår af afsnit 7.5.2.2. ovenfor, er det også efter de gældende bemærkninger til persondataloven således, at Datatilsynet udøver sin virksomhed gennem generelle retningslinjer og ved en serviceorienteret rådgivning og vejledning.

Set bl.a. i lyset af det sanktionsniveau, der fremadrettet vil være, må det imidlertid med rette kunne forventes, at der kommer meget mere fokus på denne opgave, når databeskyttelsesforordningen finder anvendelse. Tilsynsmyndigheden vil som noget nyt endvidere i forbindelse med sit informationsarbejde skulle have særlig tanke på børn ─ det kan være ved udvælgelse af emner, der skal være fokus på eller ved at lave information specielt rettet mod børn.

7.5.3.1.3. Databeskyttelsesforordningens artikel 57, stk. 1, litra c

Det fremgår af forordningens artikel 57, stk. 1, litra c, at der i henhold til medlemsstaternes nationale ret skal hver tilsynsmyndighed rådgive det nationale parlament, regeringen og andre institutioner og organer om lovgivningsmæssige og administrative foranstaltninger til beskyttelse af fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling.

Dette må anses at svare til, hvad der er gældende ret i dag, jf. persondatalovens § 57 og dens forarbejder, jf. ovenstående afsnit.

7.5.3.1.4. Databeskyttelsesforordningens artikel 57, stk. 1, litra f

Tilsynsmyndigheden skal ifølge forordningens artikel 57, stk. 1, litra f, også behandle klager, der indgives af en registreret eller af et organ, en organisation eller en sammenslutning i overensstemmelse med artikel 80, og, for så vidt det er hensigtsmæssigt, undersøge genstanden for klagen og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist, navnlig hvis yderligere undersøgelse eller koordinering med en anden tilsynsmyndighed er nødvendig.

Dette må stort set anses at svare til persondatalovens § 58, stk. 1. For så vidt angår forpligtelsen til at underrette klager om forløbet og resultatet, henvises til, at Datatilsynet er en del af den offentlige forvaltning, hvorfor tilsynet i forbindelse med sin virksomhed er omfattet af den regulering, der gælder for forvaltningsmyndigheder. Det vil bl.a. sige offentlighedsloven, forvaltningsloven og uskrevne forvaltningsretlige grundsætninger samt god forvaltningsskik.

7.5.3.1.5. Databeskyttelsesforordningens artikel 57, stk. 1, litra g og litra h

Efter forordningens artikel 57, stk. 1, litra g, skal tilsynsmyndigheden samarbejde med andre tilsynsmyndigheder, herunder gennem udveksling af oplysninger og gensidig bistand, med henblik på at sikre ensartet anvendelse og håndhævelse af denne forordning.

Tilsynsmyndigheden skal endvidere ifølge forordningens artikel 57, stk. 1, litra h, gennemføre undersøgelser om anvendelsen af denne forordning, herunder på grundlag af oplysninger, der er modtaget fra en anden tilsynsmyndighed eller en anden offentlig myndighed.

Der er allerede et vist samarbejde i dag, men samarbejdet vil fremadrettet blive langt mere formaliseret og væsentligt udbygget. Der henvises i den forbindelse til forordningens artikel 60 (”one-stop-shop”), artikel 61 og artikel 62 samt reglerne om sammenhængsmekanismen i forordningens kapitel VII (artikel 63-67).

7.5.3.1.6. Databeskyttelsesforordningens artikel 57, stk. 1, litra i

Efter forordningens artikel 57, stk. 1 litra i, skal tilsynsmyndigheden holde øje med relevant udvikling, for så vidt den har indvirkning på beskyttelse af personoplysninger, navnlig udviklingen inden for informations- og kommunikationsteknologi og handelspraksis.

Bestemmelsen er efter sin ordlyd ikke udtømmende. Forpligtelsen til at holde øje med relevant udvikling er således af generel karakter.

Der er formelt set ikke tale om en ny opgave for tilsynsmyndigheden, idet det må anses for vanskeligt for en tilsynsmyndighed at opfylde sine forpligtelser, hvis den ikke holder øje med udviklingen på området. Datatilsynet følger således også allerede i dag med i den teknologiske udvikling, hvis der er behov for dette i forbindelse med f.eks. en konkret sag, men tilsynet opsøger ikke denne type opgave. Med forordningens artikel 57, stk. 1, litra i, lægges der imidlertid op til en styrkelse af kravet om, at tilsynsmyndighederne skal holde sig ajour med udviklingen inden for informations- og kommunikationsteknologi og handelspraksis.

7.5.3.1.7. Databeskyttelsesforordningens artikel 57, stk. 1, litra j
Tilsynsmyndigheden skal efter forordningens artikel 57, stk. 1, litra j, vedtage standardkontraktbestemmelser som omhandlet i artikel 28, stk. 8, og i artikel 46, stk. 2, litra d.

Det fremgår i den forbindelse af artikel 28, stk. 8, i forordningen, at en tilsynsmyndighed kan vedtage standardkontraktbestemmelser i de tilfælde, der er omhandlet i denne artikels stk. 3 og 4, og i overensstemmelse med sammenhængsmekanismen, der er omhandlet i artikel 63. Tilsynsmyndighederne kan således fastsætte standardkontraktbestemmelser for aftaler, der skal indgås mellem den dataansvarlige og databehandleren, og for aftalen når der benyttes en underdatabehandler.

Artikel 46, stk. 2, litra d, i forordningen fastslår, at der kan ske overførsel til tredjelande, hvis der stilles fornødne garantier. Disse garantier kan bl.a. sikres gennem standardbestemmelser om databeskyttelse vedtaget af en tilsynsmyndighed og godkendt af Kommissionen efter undersøgelsesproceduren i artikel 93, stk. 2.

Datatilsynet har ikke denne adgang til at vedtage standardkontraktbestemmelser i dag, og der er derfor tale om en ny opgave.

7.5.3.1.8. Databeskyttelsesforordningens artikel 57, stk. 1, litra k og litra l
Efter forordningens artikel 57, stk. 1, litra k, skal tilsynsmyndigheden opstille og føre en liste i forbindelse med kravet om en konsekvensanalyse vedrørende databeskyttelse i henhold til artikel 35, stk. 4.

Det fremgår i den forbindelse af databeskyttelsesforordningens artikel 35, stk. 4, at tilsynsmyndigheden udarbejder og offentliggør en liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse i henhold til stk. 1. Der er tale om en ny opgave for Datatilsynet.

Tilsynsmyndigheden skal endvidere ifølge artikel 57, stk. 1, litra l, rådgive om behandlingsaktiviteter som omhandlet i artikel 36, stk. 2.

For så vidt angår artikel 36, stk. 2, så følger det heraf, at tilsynsmyndigheden skal rådgive de dataansvarlige i de tilfælde, hvor tilsynsmyndigheden får forelagt en konsekvensanalyse, fordi denne viser, at behandlingen vil medføre en høj risiko og tilsynsmyndigheden finder, at den planlagte behandling overtræder denne forordning, navnlig hvis den dataansvarlige ikke tilstrækkeligt har identificeret eller begrænset risikoen.

Der er tale om nye opgaver for tilsynsmyndigheden.

7.5.3.1.9. Databeskyttelsesforordningens artikel 57, stk. 1, litra m - q

Begrebet "adfærdskodekser" er ikke nyt, jf. persondatalovens § 74. Det har dog aldrig rigtig vundet indpas i Danmark. Med databeskyttelsesforordningen lægges der imidlertid nu op til, at der skal langt mere fokus på dette værktøj, og paletten udvides endvidere med muligheden for at opnå certificering. Forordningen indeholder således en række nye regler om adfærdskodekser og certificeringer, og tilsynsmyndigheden vil i den forbindelse få en række nye opgaver.

Tilsynsmyndigheden skal således efter forordningens artikel 57, stk. 1, litra m, tilskynde til udarbejdelse af adfærdskodekser i henhold til artikel 40, stk. 1, og afgive udtalelse om og godkende sådanne adfærdskodekser, som sikrer tilstrækkelige garantier i henhold til artikel 40, stk. 5

Endvidere skal tilsynsmyndigheden tilskynde til fastlæggelse af certificeringsmekanismer for databeskyttelse og databeskyttelsesmærkninger og -mærker i henhold til artikel 42, stk. 1, og godkende kriterierne for certificering i henhold til artikel 42, stk. 5, jf. forordningens artikel 57, stk. 1, litra n.

Tilsynsmyndigheden skal endvidere ifølge forordningens artikel 57, stk. 1, litra o, når det er relevant, regelmæssigt gennemgå certificeringer udstedt i henhold til artikel 42, stk. 7.

Herudover fastslår forordningens artikel 57, stk. 1, litra p og litra q, at tilsynsmyndigheden skal opstille og offentliggøre kriterierne for akkreditering af et organ til kontrol af adfærdskodekser i henhold til artikel 41 og af et certificeringsorgan i henhold til artikel 43 og foretage akkreditering af et organ til kontrol af adfærdskodekser i henhold til artikel 41 og af et certificeringsorgan i henhold til artikel 43.

7.5.3.1.10. Databeskyttelsesforordningens artikel 57, stk. 1, litra r og litra s

Af forordningens artikel 57, stk. 1, litra r, fremgår, at tilsynsmyndigheden skal godkende kontraktbestemmelser og bestemmelser som omhandlet i artikel 46, stk. 3, om garantier i forbindelse med overførsel af personoplysninger til et tredjeland.

Endvidere skal tilsynsmyndigheden efter forordningens artikel 57, stk. 1, litra s, i forbindelse med overførsel af oplysninger til tredjelande godkende bindende virksomhedsregler i henhold til artikel 47.

Datatilsynet varetager allerede i dag opgaven med at godkende bindende virksomhedsregler (Binding Corporate Rules – BCR).

7.5.3.1.11. Databeskyttelsesforordningens artikel 57, stk. 1, litra t
Som en af opgaverne oplistet i artikel 57, skal tilsynsmyndigheden bidrage til Databeskyttelsesrådets aktiviteter. Dette vil også fremgå af andre bestemmelser i forordningen om arbejdet i Databeskyttelsesrådet, men er også medtaget her.

Tilsynsmyndighederne samarbejder allerede i dag i regi af den såkaldte Artikel 29-gruppe, der 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.

Opgaven ændrer dog karakter, da arbejdet i Databeskyttelsesrådet er af en anden art (i Databeskyttelsesrådet vil der bl.a. skulle træffes bindende afgørelser) end det arbejde, der i dag foregår i Artikel 29-gruppen.

7.5.3.1.12. Databeskyttelsesforordningens artikel 57, stk. 1, litra u
Det fremgår af forordningens artikel 57, stk. 1, litra u, at tilsynsmyndigheden skal føre interne fortegnelser over overtrædelser af denne forordning og over foranstaltninger, der er truffet i henhold til artikel 58, stk. 2.

Der er tale om en ny opgave for Datatilsynet. Det fremgår ikke, hvilken form en sådan fortegnelse skal have. Det afgørende må imidlertid være, at oplysningerne er tilgængelige for tilsynsmyndigheden.

7.5.3.1.13. Databeskyttelsesforordningens artikel 57, stk. 1, litra v
Af forordningens artikel 57, stk. 1, litra v, fremgår, at tilsynsmyndigheden skal udføre enhver anden opgave i forbindelse med beskyttelse af personoplysninger.

Der er tale om en opsamlingsbestemmelse, som giver medlemsstaterne mulighed for at tildele deres egne tilsynsmyndigheder yderligere opgaver. Dette kan præciseres ved lovgivning eller med direkte henvisning til artiklen.

7.5.3.2. Indgivelse af klager (artikel 57, stk. 2)
Efter forordningens artikel 57, stk. 2, skal hver tilsynsmyndighed lette indgivelse af klager, jf. stk. 1, litra f, gennem foranstaltninger som f.eks. en klageformular, der også kan udfyldes elektronisk, uden at udelukke andre kommunikationsmidler.

Der er tale om en ny forpligtelse for Datatilsynet.

7.5.3.3. Udgifter i forbindelse med opgavevaretagelsen (artikel 57, stk. 3)
Af forordningens artikel 57, stk. 3, fremgår det, at hver tilsynsmyndighed varetager sine opgaver uden udgifter for den registrerede og, hvis det er relevant, for databeskyttelsesrådgiveren.

Tilsynsmyndigheden kan derfor ikke opkræve et gebyr for indgivelse af klage eller andre omkostninger i forbindelse hermed. Se dog artikel 57, stk. 4, hvor der er mulighed for at opkræve et mindre gebyr ved åbenbart grundløse eller uforholdsmæssige anmodninger.

Tilsynsmyndigheden kan heller ikke kræve betaling for eventuel rådgivning af databeskyttelsesrådgivere.

7.5.4. Overvejelser
Sammenholder man tilsynsmyndighedens "opgaveliste" i artikel 57 i databeskyttelsesforordningen med de opgaver, der kan udledes af databeskyttelsesdirektivet, persondataloven og praksis i dag, kan det konstateres, at tilsynsmyndigheden fremadrettet, når forordningen finder anvendelse fra den 25. maj 2018, vil få en del nye opgaver og forpligtelser. Der er dog også opgaver, som må antages at svare til, hvad der følger af gældende ret og praksis i dag, men som alligevel alle må forventes ændret – både i omfang og betydning.

7.6. Åbenbart grundløse eller uforholdsmæssige anmodninger, artikel 57, stk. 4

7.6.1. Præsentation
Ifølge databeskyttelsesforordningens artikel 57, stk. 4, kan tilsynsmyndigheden opkræve rimeligt gebyr for anmodninger eller afvise at efterkomme anmodninger, hvis anmodningerne er åbenbart grundløse eller uforholdsmæssige.

7.6.2. Gældende ret
Der er ikke efter gældende ret en specifik bestemmelse om, hvornår tilsynsmyndighederne (Datatilsynet og Domstolsstyrelsen) kan afvise at efterkomme en anmodning, eller opkræve et gebyr under henvisning til anmodningens omfang eller antallet af anmodninger.

7.6.2.1. Afvisning af at efterkomme anmodninger
Den nærmere ramme for, hvornår Datatilsynet og Domstolsstyrelsen kan afvise at efterkomme anmodninger, afhænger af myndighedernes kompetence og forpligtelser, som bl.a. følger af myndighedens lovgrundlag og almindelige forvaltningsretlige principper.

Anmodninger, der falder helt uden for tilsynsmyndighedernes kompetence, kan altid afvises. Dog er myndighederne forpligtet til så vidt muligt at oversende anmodningerne til rette myndighed, jf. forvaltningslovens § 7, stk. 2.

Tilsynsmyndighedernes kompetence følger bl.a. af persondatalovens § 58, stk. 1, hvorefter de af egen drift eller efter klage fra en registreret påser, at behandling af personoplysninger finder sted i overensstemmelse med persondataloven og regler udstedt i medfør af loven.

Folketingets Ombudsmand har i en sag udtalt sig om Datatilsynets muligheder for at afvise at efterkomme en anmodning om at påbegynde en undersøgelse af egen drift.[777] I sagen havde en borger klaget til ombudsmanden over, at Datatilsynet ikke mente, at der var grundlag for at indlede en generel tilsynssag vedrørende behandlingssikkerheden hos Told- og Skattestyrelsen. Ombudsmanden kunne ikke kritisere grundlaget for Datatilsynets beslutning om ikke at foretage sig yderligere i sagen.

Folketingets Ombudsmand udtalte generelt, at det forhold, at Datatilsynet ifølge persondataloven *af egen drift* eller *efter klage fra en registreret* fører tilsyn, indebærer, at alle kan klage til Datatilsynet – også selv om de ikke er registrerede og individuelt berørte af det forhold, der klages over. Datatilsynet er dog kun forpligtet til at realitetsbehandle en klage, hvis den kommer fra en registreret, som er direkte berørt af det forhold, der klages over.[778]

Endvidere udtalte Folketingets Ombudsmand, at hvis Datatilsynet modtager en klage/anmeldelse fra en person, som ikke er registreret og direkte berørt af det forhold, der klages over, kan tilsynet (af egen drift) tage det/de spørgsmål, der klages over, op som en (generel) tilsynssag, hvis der findes anledning til det. Ombudsmanden udtalte endvidere, at i visse tilfælde vil Datatilsynet være forpligtet til at tage en sag op af egen drift på baggrund af en klage/anmeldelse fra en person, som ikke er registreret og direkte berørt af det forhold, der klages over. Det er imidlertid næppe muligt præcist at angive, hvornår tilsynet vil være forpligtet, og derfor heller ikke, hvornår tilsynet kan afvise at tage en sag op. Mens det på den ene side utvivlsomt er sådan, at tilsynet ikke er forpligtet til at behandle alle klager/anmeldelser fra personer, som ikke er registrerede og direkte berørte, og som påstår, at persondataloven bliver overtrådt, så vil tilsynet på den anden side formentlig være forpligtet til at tage en sag op af egen drift, hvis der rejses en konkret begrundet mistanke om, at der er sket en lovovertrædelse af nogen betydning.[779]

---

[777] Folketingets Ombudsmands udtalelse, FOB 2007.134 (ombudsmandens sag med j.nr. 2005-2259-203).
[778] Folketingets Ombudsmands udtalelse, FOB 2007.134 (ombudsmandens sag med j.nr. 2005-2259-203), s. 30.
[779] Folketingets Ombudsmands udtalelse, FOB 2007.134 (ombudsmandens sag med j.nr. 2005-2259-203), s. 31.

På den baggrund må det generelt antages, at Datatilsynet vil kunne afvise at foretage yderligere i en sag baseret på en klage eller anmodning fra en person, som ikke er registreret eller direkte berørt af det forhold, der klages over, når det viser sig, at klagen eller anmodningen er åbenbart grundløs.

Derimod vil tilsynsmyndighederne næppe kunne afvise at foretage yderligere i en sag, hvis klagen indikerer, at der har været begrundet mistanke om, at der er sket en lovovertrædelse af nogen betydning.

7.6.2.2. Opkrævning af gebyrer

I gældende ret findes der specifikke regler om gebyrer i persondatalovens § 63, stk. 2, hvorefter der betales gebyr for privates anmeldelser og ansøgninger til Datatilsynet.

Herudover findes der ikke specifikke regler om betaling af gebyrer for anmodninger til Datatilsynet eller Domstolsstyrelsen.

Da det efter gældende ret i almindelighed vil kræve lovhjemmel for, at myndigheder kan opkræve gebyrer for at udføre deres opgaver, antages tilsynsmyndighederne ikke at have en adgang til at opkræve gebyrer for åbenbart grundløse og uforholdsmæssige anmodninger.[780]

7.6.3. Databeskyttelsesforordningen

Det følger af forordningens artikel 57, stk. 1 og stk. 3, at hver tilsynsmyndighed har en række opgaver, der som udgangspunkt skal varetages uden udgifter for den registrerede og, hvis det er relevant, for databeskyttelsesrådgiveren.

Hvis anmodninger er åbenbart grundløse eller uforholdsmæssige, især fordi de gentages, kan tilsynsmyndigheden efter forordningens artikel 57, stk. 4, imidlertid opkræve et rimeligt gebyr baseret på de administrative omkostninger *eller* afvise at efterkomme anmodningen. Ifølge bestemmelsen har tilsynsmyndigheden bevisbyrden for, at anmodningen er åbenbart grundløs eller uforholdsmæssig.

7.6.3.1. Anmodninger

Udtrykket 'anmodninger' i bestemmelsen må antages at skulle forstås bredt som henvendelser, der går ud på, at tilsynsmyndighederne skal foretage sig noget, som henhører under deres opgaver i henhold til forordningen.

[780] Jens Garde m.fl., Forvaltningsret. Almindelige emner, 6. udgave (2016), s. 194 ff.

Endvidere er det ikke et krav, at anmodningen skal komme et bestemt sted fra, f.eks. fra en registreret, for at den kan blive omfattet af bestemmelsen. Der kan således også være tale om en anmodning fra en dataansvarlig eller en borger, som ikke er registreret.

7.6.3.2. Åbenbart grundløs

En anmodning må bl.a. anses for at være *åbenbart grundløs*, hvis den ikke indeholder relevante elementer omfattet af forordningen, eller hvis anmodningen allerede på det foreliggende grundlag kan siges at være klart udsigtsløs.

7.6.3.3. Uforholdsmæssig

En anmodning må på baggrund af bestemmelsens ordlyd bl.a. anses for *uforholdsmæssig*, hvis den allerede er blevet efterkommet og herefter gentages. Bestemmelsen synes imidlertid ikke at udelukke, at anmodninger kan være uforholdsmæssige, selv om de ikke gentages. Spørgsmålet om, hvorvidt en anmodning kan anses for uforholdsmæssig, må holdes op imod de opgaver og forpligtelser, som tilsynsmyndighederne har i medfør af forordningens artikel 57, stk. 1, og formålet med tilsynet. Endvidere må styrken af den interesse, der er i, at anmodningerne imødekommes, skulle inddrages.

Er en anmodning uforholdsmæssig kan vedkommende tilsynsmyndighed således efter ordlyden af artikel 57, stk. 4, vælge at opkræve et rimeligt gebyr eller *afvise* at efterkomme anmodningen. Tilsynsmyndigheden kan således *f.eks.* inddrage ressourcehensyn ved vurderingen af, om en anmodning skal afvises. Denne afvisningsmulighed er en nyskabelse i forhold til gældende ret. Et lignende eksempel ses f.eks. i konkurrencelovens § 15, stk. 1.[781]

At tilsynsmyndigheden efter databeskyttelsesforordningen har mulighed for at afvise at behandle en klage, er i øvrigt forudsat i forordningens artikel 78, stk. 2, hvor det fremgår, at uden at det berører andre administrative eller udenretslige klageadgange, har den enkelte registrerede adgang til effektive retsmidler, hvis den tilsynsmyndighed, der er kompetent i henhold til artikel 55 og 56, *ikke behandler en klage* eller undlader at underrette den registrerede om forløbet eller resultatet af en klage, der er indgivet i henhold til artikel 77, inden for tre måneder.

Dette er også forudsat i præambelbetragtning nr. 141, hvor det bl.a. fremgår, at enhver registreret bør have ret til at indgive klage til en enkelt tilsynsmyndighed, navnlig i den medlemsstat, hvor vedkommende har sit sædvanlige opholdssted, og have adgang til effektive retsmidler i overensstemmelse med artikel 47 i chartret, hvis den registrerede finder, at

[781] Der kan også henvises til kommunestyrelseslovens § 48 a som formuleret ved ændringslov nr. 176 af 21. februar 2017.

vedkommendes rettigheder i henhold til denne forordning er blevet krænket, eller *hvis tilsynsmyndigheden ikke reagerer på en klage, delvist eller helt afslår eller afviser en klage* eller ikke handler, hvis handling er nødvendig for at beskytte den registreredes rettigheder. Derudover er dette også forudsat i præambelbetragtning nr. 143, hvor det af 5. afsnit fremgår, at en sådan afgørelse navnlig vedrører tilsynsmyndighedens udøvelse af undersøgelsesbeføjelser, korrigerende beføjelser og godkendelsesbeføjelser eller afslag eller *afvisning af klager*.

Ved valget mellem, om der skal ske afvisning eller opkræves gebyr ved en uforholdsmæssig anmodning, må det efter almindelig proportionalitets betragtninger, som er udtrykt i præambelbetragtning nr. 129, være det mindst bebyrdende for den, som har anmodet tilsynsmyndigheden, som skal foretrækkes. I den forbindelse bør der lægges vægt på udsigterne for den pågældende ved valget af det ene frem for det andet. Forekommer det eksempelvis formålsløst at opkræve gebyr og efterkomme anmodningen, bør det foretrækkes at afvise den uforholdsmæssige anmodning.

Der bør desuden så tidligt som muligt gives vejledning om, at tilsynsmyndigheden har hjemmel til at kræve gebyr.[782]

Falder vurderingen ud til, at der kan opkræves gebyr, skal gebyrets størrelse ifølge bestemmelsen være *rimelig* og være *baseret på de administrative omkostninger*. Et gebyr antages derfor ikke at måtte overstige de administrative omkostninger, som tilsynsmyndigheden med rimelighed kan forvente at skulle afholde for at efterkomme den uforholdsmæssige del af anmodningen.

Det tilføjes, at forordningens artikel 57, stk. 4, må anses for også at være en undtagelse til artikel 57, stk. 3, hvorfor sidstnævnte stykke ikke vil være til hinder for, at der opkræves gebyrer for uforholdsmæssige anmodninger fra registrerede.

Kan det *afvises* at efterkomme en anmodning, antages det kun at være den del af anmodningen, som er uforholdsmæssig, der kan afvises.

7.6.3.4. Bevisbyrde

Endelig fremgår det som nævnt af artikel 57, stk. 4, sidste pkt., at tilsynsmyndigheden har *bevisbyrden* for, at en anmodning er åbenbart grundløs eller uforholdsmæssig. Tilsynsmyndigheden skal således på tidspunktet for afvisningen af at efterkomme en anmodning

[782] Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave (2013), s. 267.

eller opkrævning af gebyr herfor kunne godtgøre, at anmodningen er åbenbart grundløs eller uforholdsmæssig.

7.6.4. Overvejelser

Forordningens artikel 57, stk. 4, er en nyskabelse i forhold til i dag. Dels er der tale om en præcisering af, hvad der allerede gælder for afvisning af at efterkomme åbenbart grundløse anmodninger i dag, mens der for opkrævning af gebyrer for og afvisning af uforholdsmæssige anmodninger må anses at være tale om en nyskabelse.

Som anført ovenfor vedrørende gældende ret antages det i dansk ret, at der i almindelighed kræves lovhjemmel for, at en myndighed kan opkræve gebyrer for at udføre deres opgaver, og gebyrets størrelse bør derfor nærmere reguleres i en ny persondatalov.

7.7. Tilsynsmyndighedens beføjelser, artikel 58

7.7.1. Præsentation

Efter databeskyttelsesforordningens artikel 58 har hver tilsynsmyndighed en række beføjelser. Udgangspunktet er, at disse beføjelser skal udøves af en tilsynsmyndighed på dens eget territorium, jf. forordningens artikel 55, stk. 1.

I det følgende gennemgås de undersøgelsesbeføjelser, korrigerende beføjelser og godkendelses- og rådgivningsbeføjelser mv., som den enkelte tilsynsmyndighed vil få efter forordningens artikel 58, stk. 1, litra a-d, artikel 58, stk. 2, og artikel 58, stk. 3-6, med de beføjelser, som Datatilsynet har efter gældende ret.

7.7.2. Gældende ret

7.7.2.1. Tilsynsmyndighedens beføjelser efter databeskyttelsesdirektivet

Databeskyttelsesdirektivet indeholder i artikel 28, stk. 3, nærmere bestemmelser om, hvilke beføjelser en tilsynsmyndighed skal tillægges i forhold til behandlinger, som finder sted på den pågældende medlemsstats område. Tilsynsmyndigheden skal bl.a. kunne:

1) 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 (artikel 28, stk. 3, 1. pind),

2) gribe effektivt ind ved f.eks. at afgive udtalelser forud for iværksættelsen af behandlinger i henhold til artikel 20 og sikre en passende offentliggø-

relse af disse udtalelser, at beordre oplysninger blokeret, slettet eller tilintetgjort, midlertidigt eller definitivt at forbyde en behandling, at udstede en advarsel til den [dataansvarlige] eller påtale en overtrædelse over for den dataansvarlige eller ved at høre parlamenter eller andre nationale politiske institutioner (artikel 28, stk. 3, 2. pind), og

3) indbringe overtrædelser af de nationale bestemmelser, som vedtages til gennemførelse af dette direktiv, for retsinstanserne eller gøre retsinstanserne opmærksom på disse overtrædelser (artikel 28, stk. 3, 3. pind).

Af Registerudvalgets betænkning nr. 1345 fremgår, at databeskyttelsesdirektivet efter udvalgets opfattelse hverken foreskriver eller udelukker, at der i den nationale lovgivning fastsættes forskellige regler vedrørende tilsynsmyndighedens beføjelser over for henholdsvis den private og den offentlige sektor. Tilsynsmyndigheden må blot antages at skulle udstyres med de beføjelser, som i fornøden grad sætter tilsynsmyndigheden i stand til at påse overholdelsen af de bestemmelser, som vedtages til gennemførelse af direktivet. Dog skal tilsynsmyndigheden som minimum kunne iværksætte undersøgelser, gribe effektivt ind samt indbringe overtrædelser for de nationale retsinstanser.[783]

Udvalget bemærker endvidere i relation til direktivets artikel 28, stk. 3, 3. pind, at den ordning, der på daværende tidspunkt var gældende for tilsynsmyndigheden (Registertilsynet), hvorefter tilsynet indbringer overtrædelser af registerlovgivningen for domstolene ved at indgive en politianmeldelse mod den, som efter tilsynets opfattelse har overtrådt lovgivningen, efter udvalgets opfattelse ikke kan antages at være i strid med direktivet, da resultatet under alle omstændigheder er, at tilsynsmyndigheden foranlediger, at bestemte forhold bliver indbragt for domstolene. Udvalget foreslog på den baggrund, at der ikke blev indsat særlige bestemmelser herom i en kommende ny lov.

Herudover fremgår det af databeskyttelsesdirektivets artikel 27, stk. 1, at medlemsstaterne og Kommissionen tilskynder til udarbejdelse af adfærdskodekser, 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 direktivet. Udkast til sådanne nationale adfærdskodekser skal kunne forelægges for den nationale tilsynsmyndighed til udtalelse, og medlemsstaterne fastsætter bestemmelser om, at tilsynsmyndigheden bl.a. skal kontrollere, at de udkast, den får forelagt, er i overensstemmelse med de nationale bestemmelser, der vedtages til gennemførelse af direktivet. Hvis myndigheden finder det

[783] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 358.

hensigtsmæssigt, kan den indhente bemærkninger fra de registrerede eller disses repræsentanter, jf. direktivets artikel 27, stk. 2.

7.7.2.2. Datatilsynets nuværende beføjelser

7.7.2.2.1. Generel tilsyns- og afgørelsesbeføjelse

Datatilsynets almindelige kompetence til at træffe afgørelse over for private – og i visse tilfælde offentlige – dataansvarlige om iagttagelse af reglerne i persondataloven følger af lovens § 55, stk. 1, hvorefter tilsynet, der består af et råd og et sekretariat, fører tilsyn med enhver behandling, der omfattes af loven. Bestemmelsen har sin baggrund i databeskyttelsesdirektivets *artikel 28, stk. 1*, og til dels *artikel 28, stk. 3, 1. pind*.

Persondatalovens § 55, stk. 1, skal i øvrigt ses i sammenhæng med lovens § 58, stk. 1, hvorefter Datatilsynet af egen drift eller efter klage fra en registreret påser, at behandlingen finder sted i overensstemmelse med loven og regler udstedt i medfør heraf. Enhver registreret person eller virksomhed mv., som er beskyttet af persondataloven, jf. lovens § 1, kan således i overensstemmelse med de almindelige forvaltningsretlige regler indgive en anmodning til Datatilsynet om beskyttelse af sine rettigheder efter loven. Herudover kan Datatilsynet tage sager op af egen drift. Tredjemand har derimod som udgangspunkt ikke en ret til at klage til Datatilsynet med den følge, at tilsynet skal behandle sagen, men tilsynet kan i sådanne tilfælde tage sagen op af egen drift, hvis der vurderes at være anledning dertil.

Datatilsynet kan endvidere efter persondatalovens § 58, stk. 2, til enhver tid tilbagekalde en afgørelse truffet i henhold til § 27, stk. 4, eller § 50, stk. 2, jf. § 27, stk. 1, eller stk. 3, nr. 2-4, hvis Kommissionen træffer afgørelse om, at der ikke må ske overførsel af oplysninger til bestemte tredjelande, eller om, at der lovligt kan ske en sådan overførsel. Dette gælder dog kun, såfremt tilbagekaldelsen er nødvendig for at efterleve Kommissionens afgørelse.

Bestemmelsen, der er indsat på baggrund af databeskyttelsesdirektivets artikel 25, stk. 4, artikel 25, stk. 6, sidste afsnit, artikel 26, stk. 3, sidste afsnit, samt artikel 26, stk. 4, giver Datatilsynet hjemmel til at tilbagekalde begunstigende afgørelser om overførsel af oplysninger til tredjelande, truffet over for såvel dataansvarlige som registrerede. Det er efter bestemmelsen en forudsætning, at tilbagekaldelsen er nødvendig for at efterleve Kommissionens afgørelse. Bestemmelsen kan imidlertid ikke antages at gøre udtømmende op med spørgsmålet om tilbagekaldelse af trufne afgørelser. Tilbagekaldelse vil således (på ulovbestemt grundlag) efter omstændighederne også kunne ske i andre situationer.

Datatilsynet kan endvidere i medfør af persondatalovens § 58, stk. 3, i særlige tilfælde forbyde eller suspendere overførsel af personoplysninger, som er omfattet af § 27, stk. 5. Be-

stemmelsen indebærer, at Datatilsynet kan forbyde eller suspendere overførsel af personoplysninger, selvom overførslen sker på grundlag af kontraktbestemmelser, der er i fuld overensstemmelse med Kommissionens standardkontraktbestemmelser.

Betingelsen i stk. 3 om, at der skal foreligge særlige tilfælde, skal forstås i overensstemmelse med artikel 4 i Kommissionens beslutning 2001/497/EF og artikel 4 i Kommissionens afgørelse af 5. februar 2010. Det følger af disse bestemmelser, at de kompetente myndigheder i medlemsstaterne skal kunne gøre brug af deres beføjelser til at forbyde eller suspendere datastrømmen til tredjelande i visse nærmere angivne tilfælde, f.eks. når en kompetent myndighed har fastslået, at dataimportøren ikke har overholdt standardkontraktbestemmelserne.

Det skal i den forbindelse nævnes, at Kommissionen ved gennemførelsesafgørelse (EU) 2016/2297 af 16. december 2016 har foretaget ændringer af artikel 4 i ovennævnte standardkontraktbestemmelser.[784] Ændringerne, der præciserer tilsynsmyndighedernes kompetence til at suspendere overførsler baseret på Kommissionens standardkontraktbestemmelser, foretages som konsekvens af EU-Domstolens udtalelse i den såkaldte Schrems-sag. I Schrems-sagen erklærede EU-Domstolen den tidligere Safe Harbor-ordning for ugyldig, idet ordningen – som muliggjorde overførsel af personoplysninger mellem EU og USA – bl.a. indskrænkede de europæiske tilsynsmyndigheders muligheder for at forbyde og suspendere overførsler for meget.

Tilsynsmyndigheden kan af egen drift indlede sag om forbud eller suspension af overførsel af oplysninger, der er omfattet af lovens § 58, stk. 3. En sådan sag kan også opstå på baggrund af indsigelse fra en registreret eller Kommissionen.

Når det gælder den offentlige forvaltning, har Datatilsynet efter persondatalovens § 60, stk. 1, kun afgørelseskompetence med bindende virkning over for andre myndigheder i relation til de regler, som specifikt er nævnt i bestemmelsen. I andre tilfælde har tilsynet alene kompetence til at afgive uforbindende udtalelser, jf. § 60, stk. 2.

Endvidere gælder i forhold til den offentlige forvaltning persondatalovens § 47, hvorefter Datatilsynet i de tilfælde, hvor tilsynet ikke kan tiltræde udførelsen af en behandling, som foretages for henholdsvis en underordnet myndighed (stk. 1) og en regional eller kommunal myndighed (stk. 2), kan forelægge sagen for henholdsvis vedkommende minister og indenrigs- og sundhedsministeren (nu økonomi- og indenrigsministeren). Forelæggelsen kan i tilfælde af uenighed foretages af såvel myndigheden som Datatilsynet, og proceduren

[784] EUT L 344 af 17. december 2016, s. 100.

vil kunne anvendes i hvilken som helst situation, hvor der er uenighed om udførelsen af en behandling, uanset om behandlingen skal forelægges Datatilsynet eller ej, jf. nærmere nedenfor.

Bestemmelsen i § 47 finder dog naturligvis ikke anvendelse i de situationer, hvor Datatilsynet i medfør af § 60, stk. 1, træffer bindende afgørelser over for vedkommende myndighed. Persondatalovens § 47, stk. 1, vil i øvrigt ikke være til hinder for, at vedkommende minister inddrages i de tilfælde, hvor en statslig myndighed ikke står i et underordnelsesforhold til den pågældende minister. I en sådan situation har den pågældende minister ikke afgørelseskompetence efter § 47 og vil kun kunne afgøre tvisten med bindende virkning, hvis dette følger af andet retsgrundlag.[785]

7.7.2.2.2. Adgang til at kræve enhver oplysning

Efter persondatalovens § 62, stk. 1, kan Datatilsynet kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

Bestemmelsen, der gælder over for både private dataansvarlige og den offentlige forvaltning, har sin baggrund i databeskyttelsesdirektivets *artikel 28, stk. 3, 1. pind*. Der er tale om en vigtig beføjelse for tilsynet i dets arbejde med at fastslå, om en given behandling falder ind under persondataloven og i givet fald udføres inden for lovens rammer, f.eks. i forbindelse med behandling af en klage fra en registreret person, der føler sig forurettet af en behandling, eller i forbindelse med sager, som Datatilsynet tager op af egen drift. Undladelse af at efterkomme Datatilsynets krav om oplysninger kan straffes efter persondatalovens § 70, stk. 1, nr. 3.

Private dataansvarliges behandlinger i strid med loven er i meget vidt omfang strafsanktioneret efter § 70. Oplysningspligten over for Datatilsynet efter § 62, stk. l, er derfor undergivet de begrænsninger, der følger af retssikkerhedslovens[786] § l, stk. 3, jf. § 10[787], om retten til ikke at inkriminere sig selv. Reglerne i retssikkerhedsloven skal ses i sammenhæng

[785] Persondataloven med kommentarer (2015), s. 588.

[786] Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter med senere ændringer.

[787] Ifølge retssikkerhedslovens § 10, stk. l, gælder en lovbestemt pligt til at meddele oplysninger til myndigheden ikke i forhold til den mistænkte, hvis der er konkret mistanke om, at en enkeltperson eller juridisk person har begået en lovovertrædelse, der kan medføre straf, medmindre det kan udelukkes, at de oplysninger, som søges tilvejebragt, kan have betydning for bedømmelsen af den formodede lovovertrædelse. Myndigheden skal efter stk. 3 vejlede den mistænkte om, at vedkommende ikke har pligt til at meddele oplysninger, som kan have betydning for bedømmelsen af den formodede lovovertrædelse. Den mistænkte kan meddele samtykke til at afgive oplysninger, og i givet fald skal dette samtykke være skriftligt og skal meddeles på et frivilligt, specifikt og informeret grundlag.

med det forbud mod selvinkriminering, som gælder i medfør af artikel 6 i Den Europæiske Menneskerettighedskonvention, der i Danmark er gennemført ved lov.[788]

7.7.2.2.3. Forudgående udtalelse fra Datatilsynet i forbindelse med visse behandlinger

I persondatalovens § 45, stk. 1, er opregnet en række behandlinger af oplysninger, der på grund af deres art, omfang og formål indebærer særlige risici for personers rettigheder eller frihedsrettigheder, jf. databeskyttelsesdirektivets artikel 20, stk. 1. Det er derfor efter lovens § 45, stk. 1, en forudsætning, at Datatilsynets udtalelse indhentes forud for, at disse former for behandling iværksættes.

Kravet om forudgående udtalelse, der kun gælder for behandlinger, som er omfattet af anmeldelsespligten i § 43, skal bl.a. ses på baggrund af direktivets *artikel 28, stk. 3, 2. pind*, der, som det fremgår ovenfor, specifikt nævner adgangen til at afgive udtalelser forud for iværksættelsen af behandlinger i henhold til artikel 20 som eksempel på en af de beføjelser, som kan tillægges tilsynsmyndigheden med henblik på at sikre, at denne er i stand til at "gribe effektivt ind".

7.7.2.2.4. Påbud og forbud

Det overordnede krav i databeskyttelsesdirektivets *artikel 28, stk. 3, 2. pind*, om, at tilsynsmyndigheden skal kunne "gribe effektivt ind" danner også baggrunden for persondatalovens § 59.

Af persondatalovens § 59, stk. 1, fremgår det således, at Datatilsynet kan påbyde en privat dataansvarlig at ophøre med en behandling, der ikke må finde sted efter denne lov, og at berigtige, slette eller blokere bestemte oplysninger, som er omfattet af en sådan behandling.

Tilsynet kan endvidere ifølge lovens § 59, stk. 2, forbyde en privat dataansvarlig at anvende en nærmere angiven fremgangsmåde i forbindelse med behandlingen af oplysninger, hvis tilsynet finder, at den pågældende fremgangsmåde medfører en væsentlig risiko for, at der behandles oplysninger i strid med loven.

Herudover kan Datatilsynet påbyde en privat dataansvarlig at træffe bestemte tekniske og organisatoriske sikkerhedsforanstaltninger mod, at der behandles oplysninger, som ikke må behandles, 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, jf. lovens § 59, stk. 3.

[788] Lov nr. 285 af 29. april 1992 om Den Europæiske Menneskerettighedskonvention med senere ændringer.

Endelig fremgår det af lovens § 59, stk. 4, at tilsynet i særlige tilfælde kan meddele databehandlere påbud eller forbud, jf. stk. 1-3.

Det er kun i særlige situationer, der er nævnt i persondatalovens § 59, at tilsynet har beføjelse til at meddele påbud og forbud. I andre tilfælde, f.eks. i sager vedrørende indsigtsret, vil Datatilsynets afgørelse gå ud på at fastslå, hvad der efter tilsynets opfattelse er retsstillingen efter loven, herunder hvilke rettigheder og pligter der tilkommer og påhviler den registrerede og den dataansvarlige virksomhed mv.

Datatilsynets kompetence efter persondatalovens § 59, stk. 1, skal i øvrigt ses i sammenhæng med lovens § 37, stk. 1, som pålægger den dataansvarlige at berigtige, slette eller blokere urigtige eller vildledende oplysninger mv., hvis en registreret person fremsætter anmodning herom. Den registrerede vil endvidere efter reglen i lovens § 37, stk. 2, kunne fremsætte anmodning om, at den dataansvarlige skal underrette tredjemand om, at videregivne oplysninger er blevet berigtiget, slettet eller blokeret. Det må anses for tvivlsomt, om lovens § 59, stk. 1, giver hjemmel for tilsynet til at pålægge en privat dataansvarlig at opfylde sin underretningsforpligtelse i lovens § 37, stk. 2.[789]

I relation til blokering af oplysninger vil Datatilsynet kunne give påbud herom under særlige betingelser. Tilsynet vil bl.a. kunne bestemme, at der skal ske blokering af oplysninger til visse formål eller i relation til bestemte modtagere. Tilsynet vil også kunne bestemme, at blokeringen ophæves, når bestemte betingelser er opfyldt.

For så vidt angår reglen i persondatalovens § 59, stk. 4, om, at Datatilsynet i særlige tilfælde også kan meddele databehandlere påbud eller forbud, bemærkes, at dette kan være relevant, hvis det ikke er muligt for tilsynet at meddele den dataansvarlige de nødvendige påbud eller forbud, f.eks. fordi det ikke er muligt at komme i kontakt med den dataansvarlige, eller hvis den dataansvarlige ikke ønsker at efterleve en afgørelse, som er truffet af tilsynet i henhold til stk. 1-3.

Det er dog en forudsætning, at der ikke er umiddelbar udsigt til, at tilsynet kan meddele den dataansvarlige sin afgørelse efter stk. 1-3 eller til, at den dataansvarlige efterlever Datatilsynets afgørelse, hvis denne allerede er truffet og meddelt den dataansvarlige. Det er endvidere en forudsætning, at den fortsatte behandling er til skade for den registrerede eller for andre, f.eks. fordi der foregår en ulovlig videregivelse eller anden ulovlig udspredelse af personoplysninger.[790]

[789] Persondataloven med kommentarer (2015), s. 630.
[790] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 59.

7.7.2.2.5. Offentliggørelse af udtalelser

Datatilsynet skal efter persondatalovens § 65 (1. pkt.) afgive en årlig beretning om sin virksomhed til Folketinget. Beretningen offentliggøres (2. pkt.). Tilsynet kan i øvrigt offentliggøre sine udtalelser (3. pkt.). Bestemmelsen har sin baggrund i databeskyttelsesdirektivets *artikel 28, stk. 3, 2. pind*, og *artikel 28, stk. 5*.

7.7.2.2.6. Kritik og henstillinger

I tillæg til de udtrykkeligt lovfæstede beføjelser har Datatilsynet også mulighed for at fremkomme med henstillinger, ligesom tilsynet udtaler kritik i varierende grader til såvel offentlige som private dataansvarlige, der efter tilsynets vurdering ikke måtte have levet op til kravene i persondataloven eller forskrifter udstedt i medfør heraf. Det samme gælder efter omstændighederne i forhold til eventuelle databehandlere.

7.7.2.2.7. Udarbejdelse af adfærdskodekser

Af persondatalovens § 74 følger, 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 persondataloven eller regler udstedt i medfør heraf.

Det fremgår af bemærkningerne til persondataloven, at der ikke følger en forpligtelse til at udarbejde (ikke-bindende) adfærdskodekser.[791] Bestemmelsen er således alene 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.

Bestemmelsen har indtil nu ikke haft nogen praktisk betydning.

7.7.3. Databeskyttelsesforordningen

Databeskyttelsesforordningen indeholder i artikel 58 en bestemmelse om, at tilsynsmyndigheden har en række beføjelser. Udgangspunktet er, at disse beføjelser skal udøves af en tilsynsmyndighed på dens eget territorium, jf. forordningens artikel 55, stk. 1.

Tilsynsmyndighedernes beføjelser er beskrevet i forordningens artikel 58, stk. 1, stk. 2 og stk. 3, hvor der sondres mellem undersøgelsesbeføjelser, korrigerende beføjelser samt godkendelses- og rådgivningsbeføjelser.

[791] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 74.

Det fremgår i den forbindelse også af præambelbetragtning nr. 129, at for at sikre ensartet tilsyn med og håndhævelse af denne forordning i hele Unionen bør tilsynsmyndighederne i hver medlemsstat have samme opgaver og effektive beføjelser, herunder undersøgelsesbeføjelser og beføjelser til at fastsætte korrigerende foranstaltninger og sanktioner samt godkendelses- og rådgivningsbeføjelser, navnlig i tilfælde af klager fra fysiske personer, og med forbehold for de retsforfølgende myndigheders beføjelser i henhold til medlemsstaternes nationale ret, til at indbringe overtrædelser af denne forordning for de judicielle myndigheder og deltage i retssager. Disse beføjelser bør også omfatte beføjelse til midlertidig eller definitivt at begrænse, herunder forbyde, behandling. Medlemsstaterne kan fastsætte andre opgaver, som vedrører beskyttelse af personoplysninger i henhold til denne forordning.

7.7.3.1. Tilsynsmyndighedens undersøgelsesbeføjelser (artikel 58, stk. 1)

7.7.3.1.1. Databeskyttelsesforordningens artikel 58, stk. 1, litra a – kræve alle oplysninger

Det fremgår af forordningens artikel 58, stk. 1, litra a, at hver tilsynsmyndighed skal kunne give såvel den dataansvarlige som databehandleren eller disses eventuelle repræsentanter påbud om at give alle oplysninger, der kræves til udførelse af myndighedens opgaver.

Som anført ovenfor følger det tilsvarende af persondatalovens § 62, stk. 1, at Datatilsynet – med de begrænsninger, der følger af selvinkrimineringsforbuddet i retssikkerhedsloven og Den Europæiske Menneskerettighedskonvention – kan kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

Forordningens artikel 58, stk. 1, litra a, ses således at videreføre gældende ret. Det forholder sig på samme måde med hensyn til de begrænsninger, der følger af forbuddet mod selvinkriminering i retssikkerhedsloven mv., jf. forordningens artikel 58, stk. 4, og forordningens præambelbetragtning nr. 129, hvoraf det bl.a. fremgår, at tilsynsmyndighedernes beføjelser bør udøves i overensstemmelse med de fornødne proceduremæssige garantier, der er fastsat i EU-retten og medlemsstaternes nationale ret, uvildigt, retfærdigt og inden for en rimelig frist.

7.7.3.1.2. Databeskyttelsesforordningens artikel 58, stk. 1, litra b – databeskyttelsesrevisioner

Af forordningens artikel 58, stk. 1, litra b, fremgår, at hver tilsynsmyndighed har beføjelse til at foretage undersøgelser i form af såkaldte databeskyttelsesrevisioner.

Forordningen indeholder ikke nogen definition af, hvad der nærmere ligger i begrebet ”databeskyttelsesrevisioner”.

Det bemærkes herved, at bestemmelsen i databeskyttelsesforordningens artikel 58, stk. 1, litra c, må ses i sammenhæng med de øvrige beføjelser, som tilsynsmyndighederne er givet med forordningen, herunder beføjelsen efter artikel 58, stk. 1, litra f, til at skaffe sig adgang til lokaler mv.

Formuleringen "undersøgelser i form af databeskyttelsesrevisioner" antages at dække over den adgang, som tilsynsmyndighederne nødvendigvis må have i forhold til den dataansvarlige og dennes eventuelle databehandlere til at foretage en kritisk gennemgang af de foreliggende oplysninger mv. – som kan være tilvejebragt via tilsynsmyndighedens øvrige beføjelser – med henblik på at kontrollere og vurdere de nærmere omstændigheder i forbindelse med de databehandlinger, der er genstand for en given revision.

Under de angivne forudsætninger ses denne beføjelse til dels at være en kodificering, men ikke en nyskabelse i forhold til den generelle tilsynsbeføjelse, der følger af persondatalovens § 55, stk. 1, og § 58, stk. 1, jf. gennemgangen ovenfor.

7.7.3.1.3. Databeskyttelsesforordningens artikel 58, stk. 1, litra c – revision af certificeringer

Forordningens artikel 58, stk. 1, litra c, giver hver tilsynsmyndighed beføjelse til at foretage revision af certificeringer udstedt i henhold til forordningens artikel 42, stk. 7.

Forordningens artikel 42, stk. 7, fastslår, 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. Certificering trækkes tilbage af certificeringsorganerne, jf. forordningens artikel 43, eller i givet fald den kompetente tilsynsmyndighed, hvis kravene til certificering ikke er eller ikke længere er opfyldt.

Persondataloven indeholder ikke regler om certificering, hvorfor denne beføjelse til at foretage revision af sådanne, der hermed tildeles tilsynsmyndigheden, udgør en nyskabelse i forhold til gældende ret.

7.7.3.1.4. Databeskyttelsesforordningens artikel 58, stk. 1, litra d – underretning

Efter forordningens artikel 58, stk. 1, litra d, skal hver tilsynsmyndighed kunne underrette den dataansvarlige eller databehandleren om en påstået overtrædelse af forordningen.

Denne beføjelse må antages at svare til den adgang, som Datatilsynet har – som led i den generelle tilsynsforpligtelse efter persondatalovens § 55, stk. 1, og § 58, stk. 1, – til at un-

derrette den dataansvarlige eller databehandleren om en påstået overtrædelse af persondataloven, uanset om påstanden om overtrædelse hidrører fra en registreret, fra en tredjemand eller fra tilsynsmyndigheden selv. I øvrigt er Datatilsynets underretningsadgang i afgørelsessager i vidt omfang pligtmæssig i medfør af forvaltningslovens regler om partshøring.

7.7.3.2. Korrigerende beføjelser (artikel 58, stk. 2)

7.7.3.2.1. Databeskyttelsesforordningens artikel 58, stk. 2, litra a – advarsler

Af forordningens artikel 58, stk. 2, fremgår det, at hver tilsynsmyndighed skal kunne udstede advarsler til en dataansvarlig eller en databehandler om, at planlagte behandlingsaktiviteter sandsynligvis vil være i strid med denne forordning.

Persondataloven indeholder ikke en tilsvarende bestemmelse. En sådan beføjelse må dog antages at gælde bl.a. på baggrund af den generelle tilsynsforpligtelse efter lovens § 55, stk. 1, samt § 58, stk. 1, jf. ovenfor.

Hertil kommer, at Datatilsynet som led i administrationen af persondatalovens anmeldelses- og tilladelsesordninger[792] tilkendegiver over for anmelder/ansøger, hvis den påtænkte behandling efter tilsynets opfattelse vil være i strid med loven, herunder i form af egentlige afgørelser (afslag på ansøgninger om tilladelse). Der kan i den forbindelse også henvises til persondatalovens § 45.

Forordningens artikel 58, stk. 2, litra a, ses på denne baggrund ikke at tillægge tilsynsmyndighederne beføjelser i videre omfang end efter persondataloven.

7.7.3.2.2. Databeskyttelsesforordningens artikel 58, stk. 2, litra b – udtale kritik

Hver tilsynsmyndighed skal ifølge forordningens artikel 58, stk. 2, litra b, kunne udtale kritik af en dataansvarlig eller en databehandler, hvis behandlingsaktiviteter har været i strid med denne forordning.

Som nævnt ovenfor har Datatilsynet også i dag (på ulovbestemt grundlag) mulighed for at udtale kritik af såvel offentlige som private dataansvarlige samt efter omstændighederne af disses databehandlere i forhold til foretagne behandlinger af personoplysninger, som efter tilsynets vurdering ikke har levet op til kravene i persondataloven eller forskrifter udstedt i medfør heraf.

[792] Se nærmere persondatalovens kapitel 12, 13 og 14 om anmeldelse af visse behandlinger til Datatilsynet og om indhentelse af tilsynets udtalelse eller tilladelse til den anmeldte behandling samt lovens § 10, stk. 3, hvorefter visse oplysninger kun må videregives efter forudgående tilladelse fra tilsynsmyndigheden.

Databeskyttelsesforordningens artikel 58, stk. 2, litra b, kan på den baggrund ses som en kodificering af Datatilsynets nuværende praksis.

7.7.3.2.3. Databeskyttelsesforordningens artikel 58, stk. 2, litra c-g – påbud og forbud
Efter forordningens artikel 58, stk. 2, litra c, skal hver tilsynsmyndighed kunne pålægge den dataansvarlige eller databehandleren at imødekomme den registreredes anmodninger om at udøve sine rettigheder i henhold til »denne forordning«. Med udtrykket denne forordning må også forstås nationale særregler fastsat i overensstemmelse med forordningen.

Hver tilsynsmyndighed skal endvidere ifølge artikel 58, stk. 1, litra d, kunne give den dataansvarlige eller databehandleren påbud om at bringe behandlingsaktiviteter i overensstemmelse med bestemmelserne i denne forordning, og hvis det er hensigtsmæssigt, på en nærmere angivet måde og inden for en nærmere angivet frist.

Herudover skal hver tilsynsmyndighed efter artikel 58, stk. 2, litra e, kunne give den dataansvarlige påbud om at underrette den registrerede om et brud på persondatasikkerheden.

Det følger endvidere af forordningens artikel 58, stk. 2, litra f, at hver tilsynsmyndighed skal have mulighed for midlertidigt eller definitivt at begrænse, herunder forbyde, behandling, ligesom den skal kunne give påbud om berigtigelse eller sletning af personoplysninger eller begrænsning af behandling i henhold til artikel 16, 17 og 18 og meddelelse af sådanne handlinger til de modtagere, som personoplysningerne er videregivet til i henhold til artikel 17, stk. 2, og artikel 19, jf. forordningens artikel 58, stk. 2, litra g.

Indledningsvis bemærkes, at det må antages, at de i databeskyttelsesforordningens artikel 58, stk. 2, litra c-g omhandlede beføjelser om forbud og påbud – som det også er tilfældet efter persondataloven – skal forstås som beføjelser, der går videre end blot at fastlægge, hvad der efter tilsynsmyndighedens opfattelse er retsstillingen efter loven. Der er altså tale om en beføjelse til at *pålægge* modtageren af et påbud eller forbud at foretage noget aktivt i forhold til en given behandling af personoplysninger, herunder eventuelt at bringe behandlingen til ophør.

Da Datatilsynets beføjelser til at meddele egentlige påbud og forbud efter persondataloven som nævnt ovenfor kun gælder i forhold til private og kun i de situationer, der er nævnt i lovens § 59, vil forordningens artikel 58, stk. 2, litra c-g, indebære en betydelig udvidelse af tilsynets beføjelser i forhold til gældende ret.

Datatilsynet vil således som noget nyt også kunne meddele påbud til offentlige myndigheder. Herudover vil der efter artikel 58, stk. 2, litra c, kunne meddeles påbud om imøde-

kommelse af registreredes anmodninger om at udøve *alle* deres rettigheder efter forordningen, hvor Datatilsynets kompetence efter persondatalovens § 59, stk. 1, er begrænset til retten til at få slettet, berigtiget eller blokeret oplysninger.

Endelig ses der ikke med forordningen at gælde nogen særlig begrænsning i forhold til databehandlere. En retstilstand i overensstemmelse med persondatalovens § 59, stk. 4, hvorefter tilsynet alene i særlige tilfælde kan meddele databehandlere påbud eller forbud efter stk. 1-3 må derfor heller ikke forventes at kunne opretholdes.

7.7.3.2.4. Databeskyttelsesforordningens artikel 58, stk. 2, litra h – certificering
Af forordningens artikel 58, stk. 1, litra h, fremgår, at hver tilsynsmyndighed skal kunne trække en certificering tilbage eller give et certificeringsorgan påbud om at trække en certificering, der er udstedt i henhold til artikel 42 og 43, tilbage eller give certificeringsorganet påbud om ikke at udstede en certificering, hvis kravene til certificering ikke er eller ikke længere er opfyldt.

Persondataloven indeholder ikke regler om certificering, hvorfor også de beføjelser, der ifølge databeskyttelsesforordningens artikel 58, stk. 2, litra h, på dette område tillægges hver tilsynsmyndighed, udgør en nyskabelse i forhold til gældende ret. Der henvises til afsnit 5.24. om certificering, artikel 42.

7.7.3.2.5. Databeskyttelsesforordningens artikel 58, stk. 2, litra i – administrative bøder
Af forordningens præambelbetragtning nr. 151 fremgår bl.a., at retssystemet i Danmark ikke giver mulighed for administrative bøder som fastsat i forordningen, og at reglerne om administrative bøder i Danmark kan anvendes ved, at bøder pålægges af de kompetente nationale domstole som en strafferetlig sanktion, forudsat at en sådan anvendelse af reglerne i Danmark har en virkning, der svarer til virkningen af administrative bøder, som tilsynsmyndigheden pålægger. De kompetente nationale domstole bør derfor tage hensyn til en anbefaling fra den tilsynsmyndighed, der har taget skridt til en bøde. De pålagte bøder bør under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Det er i overensstemmelse hermed fastsat i forordningens artikel 83, stk. 9, at hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, kan denne artikel anvendes på en sådan måde, at den kompetente tilsynsmyndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af tilsynsmyndighederne. Bøder skal under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Den beføjelse, der i forordningens artikel 58, stk. 2, litra i, tillægges hver tilsynsmyndighed i forhold til at kunne pålægge en administrativ bøde mv. vil således ikke finde anvendelse i Danmark.

Der henvises i øvrigt til afsnit 9.10 og 9.11 om administrative bøder og sanktioner, artikel 83 og 84.

7.7.3.2.6. Suspension af overførsel af oplysninger (artikel 58, stk. 2, litra j)

Ifølge forordningens artikel 58, stk. 2, litra j, skal hver tilsynsmyndighed kunne påbyde suspension af overførsel af oplysninger til en modtager i et tredjeland eller til en international organisation.

Som anført ovenfor følger det af persondatalovens § 58, stk. 2, at tilsynet til enhver tid kan tilbagekalde en afgørelse truffet i henhold til § 27, stk. 4, eller § 50, stk. 2, jf. § 27, stk. 1, eller stk. 3, nr. 2-4, hvis Kommissionen træffer afgørelse om, at der ikke må ske overførsel af oplysninger til bestemte tredjelande, eller om, at der lovligt kan ske en sådan overførsel. Dette gælder dog kun, hvis tilbagekaldelsen er nødvendig for at efterleve Kommissionens afgørelse.

Bestemmelsen, der har baggrund i databeskyttelsesdirektivet, antages imidlertid ikke at gøre udtømmende op med spørgsmålet om tilbagekaldelse af trufne afgørelser. Tilbagekaldelse vil efter omstændighederne også kunne ske i andre situationer på ulovbestemt grundlag.[793]

Det følger endvidere af persondatalovens § 58, stk. 3, som også har baggrund i databeskyttelsesdirektivet, at tilsynsmyndigheden i særlige tilfælde kan forbyde eller suspendere overførsel af personoplysninger, som er omfattet af § 27, stk. 5 (om standardkontraktbestemmelser, som er godkendt af Kommissionen).

Betingelsen i stk. 3 om, at der skal foreligge særlige tilfælde, skal som nævnt forstås i overensstemmelse med artikel 4 i Kommissionens beslutning 2001/497/EF og artikel 4 i Kommissionens afgørelse af 5. februar 2010, hvoraf det følger, at de kompetente myndigheder i medlemsstaterne skal kunne gøre brug af deres beføjelser til at forbyde eller suspendere datastrømmen til tredjelande i visse nærmere angivne tilfælde, f.eks. når en kompetent myndighed har fastslået, at dataimportøren ikke har overholdt standardkontraktbestemmelserne.

[793] Se herom Persondataloven med kommentarer (2015), s. 628.

Under disse forudsætninger synes tilsynsmyndighedernes beføjelse efter artikel 58, stk. 2, litra j, i relation til overførsler til tredjelande i vidt omfang at svare til gældende ret. Dog giver bestemmelsen efter sin ordlyd alene hver tilsynsmyndighed en beføjelse til at påbyde *suspension* af de omhandlede overførsler, hvilket synes at udgøre en indskrænkning i forhold til persondatalovens § 58, stk. 3, der giver adgang til at *forbyde eller suspendere* (visse) overførsler.

På den anden side kan det ikke udelukkes, at der – afhængig af den fremtidige praktiske anvendelse af forordningen – kan blive tale om en udvidelse af det danske Datatilsyns beføjelse til at tilbagekalde afgørelser i videre omfang, end det gælder i dag efter persondatalovens § 58, stk. 2, og på ulovbestemt grundlag. Endvidere kan der være tale om en udvidelse i forhold til beføjelsen til at suspendere en overførsel på baggrund af standardkontrakter efter persondatalovens § 58, stk. 3, idet suspensionsbeføjelsen efter forordningen ikke synes at være begrænset til "særlige tilfælde".

I det omfang forordningens regulering af *overførsler til internationale organisationer* er nyskabende i forhold til persondataloven, vil også tilsynsmyndighedernes beføjelser herom efter artikel 58, stk. 2, litra j, være nye.

7.7.3.3. Godkendelses- og rådgivningsbeføjelser (artikel 58, stk. 3)

7.7.3.3.1. Databeskyttelsesforordningens artikel 58, stk. 3, litra a – konsekvensanalyser

Det fremgår af forordningens artikel 58, stk. 3, litra a, at hver tilsynsmyndighed skal have beføjelse til at rådgive den dataansvarlige efter den procedure for forudgående høring, der er omhandlet i artikel 36.

Efter forordningens artikel 36, stk. 1, skal den dataansvarlige høre tilsynsmyndigheden inden behandling, hvis en konsekvensanalyse vedrørende databeskyttelse efter artikel 35 viser, at behandlingen medfører en høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen. Af artikel 36, stk. 2, fremgår endvidere bl.a., at tilsynsmyndigheden, hvis denne finder, at den planlagte behandling omhandlet i stk. 1 overtræder forordningen, navnlig hvis den dataansvarlige ikke tilstrækkeligt har identificeret eller begrænset risikoen, skal give den dataansvarlige og, hvor det er relevant, databehandleren skriftlig rådgivning og kan i den forbindelse anvende enhver af sine beføjelser, jf. artikel 58.

Persondataloven indeholder ikke regler om konsekvensanalyser, hvorfor tilsynsmyndighedernes beføjelse til at rådgive i forbindelse hermed udgør en nyskabelse i forhold til gældende ret.

7.7.3.3.2. Databeskyttelsesforordningens artikel 58, stk. 3, litra b – rådgivning af parlament mv.

Ifølge forordningens artikel 58, stk. 3, litra b, skal tilsynsmyndigheden have beføjelse til på eget initiativ eller på anmodning at afgive udtalelser til det nationale parlament, medlemsstatens regering eller i overensstemmelse med medlemsstaternes nationale ret til andre institutioner og organer samt offentligheden om ethvert spørgsmål om beskyttelse af personoplysninger.

Det fremgår af forarbejderne til persondataloven, at Datatilsynet i første række bør tage sigte på at kunne udøve din virksomhed gennem generelle retningslinjer og ved en serviceorienteret rådgivning og vejledning frem for en regulering primært koncentreret om afgørelse af enkeltsager i et traditionelt rekurssystem. Som følge heraf må det antages, at Datatilsynet allerede har den beføjelse, som er nævnt i forordningens artikel 58, stk. 3, litra b.

7.7.3.3.3. Databeskyttelsesforordningens artikel 58, stk. 3, litra c – godkendelse af visse behandlinger

Hver tilsynsmyndighed skal efter forordningens artikel 58, stk. 3, litra c, have beføjelse til at godkende den type behandling, der er omtalt i artikel 36, stk. 5, hvis en sådan forudgående godkendelse er påkrævet i henhold til den pågældende medlemsstats nationale ret.

Det fremgår i den forbindelse af forordningens artikel 36, stk. 5, at det i medlemsstaternes nationale ret kan 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.

Den forudgående godkendelsesbeføjelse, der med forordningen skal tildeles hver tilsynsmyndighed, hvis medlemsstaten i sin nationale ret stiller krav herom i forhold til visse behandlinger, må antages at svare til persondatalovens § 45, som er nærmere omtalt ovenfor.

Forordningens artikel 58, stk. 2, litra a, ses på denne baggrund ikke at tillægge tilsynsmyndighederne beføjelser i videre omfang end efter persondataloven.

7.7.3.3.4. Databeskyttelsesforordningens artikel 58, stk. 3, litra d-f – adfærdskodeks og certificering

Efter forordningens artikel 58, stk. 3, litra d, skal hver tilsynsmyndighed have beføjelse til at afgive udtalelse og godkende forslag til adfærdskodekser i henhold til artikel 40, stk. 5.

Hver tilsynsmyndighed skal endvidere have beføjelse til at akkreditere (godkende) certificeringsorganer i henhold til artikel 43, ligesom den selv skal kunne udstede certificeringer og godkende kriterier for certificering i overensstemmelse med artikel 42, stk. 5, jf. forordningens artikel 58, stk. 3, litra e og litra f.

Begrebet "adfærdskodekser" er ikke nyt, idet der som nævnt ovenfor allerede i dag er mulighed for at udarbejde sådanne, jf. persondatalovens § 74. Med databeskyttelsesforordningen lægges der imidlertid som noget nyt op til, at der skal være langt mere fokus på dette værktøj, og paletten udvides endvidere med muligheden for at opnå certificering. Forordningen indeholder således en række nye regler om adfærdskodekser og certificeringer, og tilsynsmyndigheden vil i den forbindelse få en række nye opgaver og beføjelser.

7.7.3.3.5. Databeskyttelsesforordningens artikel 58, stk. 3, litra g - standardbestemmelser
Ifølge forordningens artikel 58, stk. 3, litra h, skal hver tilsynsmyndighed have beføjelse til at vedtage standardbestemmelser om databeskyttelse som omhandlet i artikel 28, stk. 8, og i artikel 46, stk. 2, litra d.

Det fremgår i den forbindelse af artikel 28, stk. 8, i forordningen, at en tilsynsmyndighed kan vedtage standardkontraktbestemmelser i de tilfælde, der er omhandlet i denne artikels stk. 3 og 4, og i overensstemmelse med sammenhængsmekanismen, der er omhandlet i artikel 63. Tilsynsmyndighederne kan således fastsætte standardkontraktbestemmelser for aftaler, der skal indgås mellem den dataansvarlige og databehandleren og dennes eventuelle underdatabehandler.

Artikel 46, stk. 2, litra d, i forordningen fastslår, at der kan ske overførsel til tredjelande, hvis der stilles fornødne garantier. Disse garantier kan bl.a. sikres gennem standardbestemmelser om databeskyttelse vedtaget af en tilsynsmyndighed og godkendt af Kommissionen efter undersøgelsesproceduren i artikel 93, stk. 2.

Datatilsynet har ikke denne adgang til at vedtage standardkontraktbestemmelser i dag, og der er derfor tale om en ny beføjelse.

7.7.3.3.5. Databeskyttelsesforordningens artikel 58, stk. 3, litra h-j – overførsel til tredjelande
Hver tilsynsmyndighed skal efter forordningens artikel 58, stk. 3, litra h og litra i, have beføjelse til at godkende kontraktbestemmelser og administrative ordninger som omhandlet i artikel 46, stk. 3, litra a og litra b, om garantier i forbindelse med overførsel af personoplysninger til et tredjeland.

Endvidere skal hver tilsynsmyndighed efter forordningens artikel 58, stk. 3, litra j, udstyres med en beføjelse til – også i forbindelse med overførsel af oplysninger til tredjelande – at godkende bindende virksomhedsregler i henhold til artikel 47.

Datatilsynet varetager allerede i dag opgaven med at godkende bindende virksomhedsregler (Binding Corporate Rules – BCR), og som det er tilfældet med de beføjelser, der er nævnt ovenfor, vurderes det således ikke, at der med forordningen tildeles tilsynsmyndigheden nye beføjelser på dette område.

7.7.3.4. Databeskyttelsesforordningens artikel 58, stk. 4 - fornødne garantier
Efter forordningens artikel 58, stk. 4, er udøvelse af de beføjelser, der tillægges tilsynsmyndigheden i medfør af denne artikel, underlagt de fornødne garantier, herunder effektive retsmidler og retfærdig procedure, der er fastsat i EU-retten eller medlemsstaternes nationale ret i overensstemmelse med chartret.

Herom er i præambelbetragtning nr. 129 endvidere anført, at tilsynsmyndighedernes beføjelser bør udøves i overensstemmelse med de fornødne proceduremæssige garantier, der er fastsat i EU-retten og medlemsstaternes nationale ret, uvildigt, retfærdigt og inden for en rimelig frist. Hver foranstaltning bør især være passende, nødvendig og forholdsmæssig for at sikre overholdelse af denne forordning, idet der tages hensyn til omstændighederne i hver enkelt sag, bør overholde enhver persons ret til at blive hørt, inden der træffes en individuel foranstaltning, som vil berøre den pågældende negativt, og bør undgå overflødige udgifter og urimelige ulemper for de berørte personer.

Forordningens artikel 58, stk. 4, indeholder ikke noget nyt set i forhold til, at Datatilsynet er en del af den offentlige forvaltning og dermed i forbindelse med sin virksomhed er omfattet af den regulering, der gælder for forvaltningsmyndigheder. Det vil bl.a. sige offentlighedsloven, forvaltningsloven og uskrevne forvaltningsretlige grundsætninger samt god forvaltningsskik.

7.7.3.5. Databeskyttelsesforordningens artikel 58, stk. 5 - indbringelse for domstolene
Hver medlemsstat skal efter forordningens artikel 58, stk. 5, ved lov fastsætte regler om, at dens tilsynsmyndighed har beføjelse til at indbringe overtrædelser af forordningen for de judicielle myndigheder og om nødvendigt at indlede eller på anden måde deltage i retssager med henblik på at håndhæve bestemmelserne i forordningen.

Som det fremgår ovenfor indeholder databeskyttelsesdirektivet i artikel 28, stk. 3, 3. pind, en tilsvarende bestemmelse. Registerudvalget fandt i den forbindelse, at den ordning, der på daværende tidspunkt var gældende for tilsynsmyndigheden (Registertilsynet), hvorefter

tilsynet indbringer overtrædelser af registerlovgivningen for domstolene ved at indgive en politianmeldelse mod den, som efter tilsynets opfattelse har overtrådt lovgivningen, efter udvalgets opfattelse ikke kan antages at være i strid med direktivet, da resultatet under alle omstændigheder er, at tilsynsmyndigheden foranlediger, at bestemte forhold bliver indbragt for domstolene. Udvalget foreslog på den baggrund, at der ikke blev indsat særlige bestemmelser herom i en kommende lov. Der henvises i øvrigt artikel 83 om administrative bøder.

7.7.3.6. Databeskyttelsesforordningens artikel 58, stk. 6 – mulighed for yderligere beføjelser

Efter forordningens artikel 58, stk. 6, fastsætter hver medlemsstat ved lov, at dens tilsynsmyndighed har yderligere beføjelser end dem, der er omhandlet i stk. 1, 2 og 3. Udøvelsen af disse beføjelser må ikke hindre en effektiv anvendelse af kapitel VII om sammenhængsmekanismen.

Der er tale om en opsamlingsbestemmelse, som giver medlemsstaterne mulighed for at tildele deres egne tilsynsmyndigheder yderligere beføjelser inden for de rammer, som en effektiv anvendelse af reglerne om sammenhængsmekanismen opstiller.

7.7.4. Overvejelser

En del af de beføjelser, som tilsynsmyndigheden har ifølge forordningens artikel 58, har Datatilsynet allerede i dag.

Dette gælder dog ikke fuldt ud forordningens artikel 58, stk. 2, litra c-g om påbud og forbud, der som nævnt vil indebære en betydelig udvidelse af tilsynets beføjelser i forhold til gældende ret.

Endvidere er det nyt, når der med databeskyttelsesforordningen lægges op til, at der skal langt mere fokus på adfærdskodekser og certificeringer, og de nye regler herom vil således indebære, at tilsynsmyndigheden på dette område vil få en række nye opgaver og beføjelser.

Der sker herudover også en udvidelse af tilsynsmyndighedens beføjelser på området overførsler til tredjeland.

Endelig skal det overvejes, om det ønskes at tillægge tilsynsmyndigheden(erne) yderligere beføjelser.

7.8. Adgang til oplysninger og lokaler, artikel 58, stk. 1, litra e og f

7.8.1. Præsentation

Databeskyttelsesforordningens artikel 58, stk. 1, litra e og f, giver tilsynsmyndighederne beføjelse til hos den dataansvarlige eller databehandleren at få adgang til alle oplysninger og lokaler mv.

I persondataloven findes reglerne om Datatilsynets adgang til oplysninger og lokaler i persondatalovens § 62.

7.8.2. Gældende ret

7.8.2.1. Datatilsynets adgang til oplysninger og lokaler mv.

Bestemmelserne i persondatalovens § 62 har sin baggrund i databeskyttelsesdirektivets artikel 28, stk. 3, 1. pind, hvorefter 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. Direktivet forholder sig ikke direkte til spørgsmålet om, hvorvidt inspektionerne skal kunne ske uden retskendelse, men direktivet lægger op til, at det hidtidige beskyttelsesniveau skal opretholdes.

Det fremgår af persondatalovens § 62, stk. 1, 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.

Det fremgår endvidere af persondatalovens § 60, stk. 2, at tilsynets medlemmer og personale til enhver tid mod behørig legitimation uden retskendelse har adgang til alle lokaler, hvorfra en behandling, som foretages for den offentlige forvaltning, administreres, eller hvorfra der er adgang til de oplysninger, som behandles, samt til lokaler, hvor oplysningerne eller tekniske hjælpemidler opbevares eller anvendes.

Af bemærkningerne til persondatalovens § 62, stk. 2, fremgår det, at bestemmelsen, som tager sigte på behandlinger, der *foretages for den offentlige forvaltning*, svarer til lov om offentlige myndigheders registre § 26, stk. 2. [794] Endvidere fremgår det, at det følger af direktivets artikel 28, stk. 3, 1. pind, at tilsynsmyndigheden skal kunne have adgang til de oplysninger, der gøres til genstand for en behandling. Det forudsættes således, at tilsynet har mulighed for selv at gøre sig bekendt med oplysningerne efter at have fået adgang til lokaler, hvorfra der er adgang til disse.

[794] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 62.

Det fremgår af persondatalovens § 60, stk. 3, at bestemmelsen i stk. 2 tilsvarende gælder for behandlinger, som foretages for private dataansvarlige, i det omfang behandlingen er omfattet af § 50 eller foretages i forbindelse med tv-overvågning.

Af bemærkningerne til § 62, stk. 3, fremgår det, at bestemmelsen, som tager sigte på behandlinger, der *foretages for private dataansvarlige*, i en vis grad svarer til lov om private registre § 22, stk. 3. [795] I bestemmelsen er fastsat en *begrænset inspektionsbeføjelse*, nemlig til de typer af behandlinger, som er undergivet et krav om forudgående tilladelse.

Det fremgår af persondatalovens § 60, stk. 4, at bestemmelsen i stk. 2 også gælder, for så vidt angår den behandling, der udføres af databehandlere som nævnt i § 53.

Endelig fremgår det af bemærkningerne til § 64, stk. 4, at bestemmelsen afløser lov om private registre § 22, stk. 3, jf. § 20, idet den dog tillige gælder for offentlige edb-servicebureauer. Der vil efter bestemmelsen kunne foretages inspektion i forhold til såvel behandlinger, der er omfattet af persondataloven, som i forhold til behandlinger, som er omfattet af en anden medlemsstats lovgivning, jf. herved § 64, stk. 1.

For Domstolsstyrelsens udøvelse af tilsyn med behandling af oplysninger, der foretages for domstolene, gælder bestemmelserne i § 62, stk. 1, 2 og 4 tilsvarende, jf. lovens § 68, stk. 1.

7.8.2.2. Forvaltningens anvendelse af tvangsindgreb

I retssikkerhedsloven[796] reguleres dels myndighedernes fremgangsmåde ved gennemførelse af tvangsindgreb, dels borgernes og virksomhedernes retsstilling, hvis der i tilknytning til tvangsindgreb opstår spørgsmål om, hvorvidt den pågældende har begået en lovovertrædelse, som kan medføre straf. Disse regler skal iagttages i forbindelse med Datatilsynets anvendelse af sine beføjelser i henhold til persondatalovens § 62.

7.8.2.2.1. Husundersøgelse mv.

Det fremgår af retssikkerhedslovens § 1, stk. 1, at lovens kapitel 2 og 3 finder anvendelse ved tvangsindgreb, som foretages af den offentlige forvaltning, og som består i *husundersøgelse* samt *undersøgelse eller beslaglæggelse af breve og andre papirer*. Det fremgår af lovforslaget, der førte til retssikkerhedsloven[797], at dette sigter til visse af de indgreb, der er omfattet af grundlovens § 72. "Husundersøgelser" omfatter således undersøgelse af private

[795] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 62.

[796] Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter med senere ændringer

[797] Forslag nr. L 96 fremsat den 26. november 2003 til lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter, de specielle bemærkninger til § 1.

lokaliteter, som anvendes til beboelse. Herudover omfatter bestemmelsen andre rum, der ikke er offentligt tilgængelige som f.eks. fabriks- og lagerlokaler, baglokaler til butikker mv., garager, stalde, lader og kahytsrum. Det fremgår desuden, at "undersøgelse eller beslaglæggelse af breve og andre papirer" omfatter enhver rådighedsberøvelse og undersøgelse af private notater, forretningspapirer, regnskaber, protokoller, logbøger og lignende. Det gælder, hvad enten de pågældende oplysninger mv. findes i papirform eller elektronisk form.

Når Datatilsynet i medfør af persondatalovens § 62, stk. 1, gennemfører inspektioner omfattet af begrebet "husundersøgelser" i retssikkerhedslovens § 1, stk. 1, nr. 1, og når tilsynet i forbindelse med afholdelse af inspektioner undersøger registre mv., vil dette være omfattet af retssikkerhedslovens § 1, stk. 1, nr. 2. Datatilsynet skal således iagttage proportionalitetsprincippet i retssikkerhedslovens § 2, samt reglerne for fremgangsmåden i retssikkerhedslovens §§ 3-8, og bestemmelsen i retssikkerhedslovens § 9 om forholdet til strafferetsplejen ved gennemførelse af tvangsindgreb.

7.8.2.2.2. Retten til ikke at inkriminere sig selv mv.
Retten til ikke at inkriminere sig selv følger bl.a. af retssikkerhedslovens § 10, hvoraf det fremgår, 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.

Retten til ikke at inkriminere sig selv har således betydning for anvendelsen af oplysningspligten i persondatalovens § 62, stk. 1.

For nærmere herom henvises til afsnit 5.11. om anmeldelse af brud på sikkerheden, artikel 33.

7.8.3. Databeskyttelsesforordningen

7.8.3.1. Tilsynsmyndighedernes adgang til oplysninger og lokaler mv.
Efter databeskyttelsesforordningens artikel 58, stk. 1, har hver tilsynsmyndighed alle de undersøgelsesbeføjelser, der er oplistet i bestemmelsen.

Hver tilsynsmyndighed har således beføjelse til i medfør af artikel 58, stk. 1, litra e, af den dataansvarlige eller databehandleren at få *adgang til alle personoplysninger og oplysninger*, der er nødvendige for at varetage dens opgaver, og i medfør af artikel 58, stk. 1, litra f,

at få *adgang til alle lokaler* hos den dataansvarlige og databehandleren, herunder databehandlingsudstyr og -midler, *i overensstemmelse med retsplejeregler* i EU-retten eller medlemsstaternes nationale ret.

Tilsynsmyndigheden skal således både have adgang til oplysninger og til lokaler. Som anført ovenfor under afsnit 7.8.2. om gældende ret har det hidtil været antaget, at det i databeskyttelsesdirektivets artikel 28, stk. 3, 1. pind – hvorefter tilsynsmyndigheden 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 – er forudsat, at tilsynet har mulighed for selv at gøre sig bekendt med oplysninger efter at have fået adgang til lokaler.

Som noget nyt fremgår det nu udtrykkeligt af forordningen, at tilsynsmyndigheden skal have *adgang til lokaler*.

Samlet set må det antages, at tilsynsmyndigheden også fremadrettet vil kunne foretage "inspektioner/tilsynsbesøg" på samme vis, som det gælder efter persondataloven. Det vil sige både fysiske inspektioner hos den dataansvarlige eller databehandleren, men også f.eks. skrivebordskontroller ved hjælp af spørgeskema eller lignende.

7.8.3.2. Tilsynsmyndighedernes anvendelse af beføjelser

Det fremgår bl.a. af forordningens præambelbetragtning nr. 129, at tilsynsmyndighedernes beføjelser bør udøves i overensstemmelse med de fornødne proceduremæssige garantier, der er fastsat i EU-retten og medlemsstaternes nationale ret, uvildigt, retfærdigt og inden for en rimelig frist. Det fremgår desuden, at hver foranstaltning især bør være passende, nødvendig og forholdsmæssig for at sikre overholdelse af forordningen, idet der tages hensyn til omstændighederne i hver enkelt sag, bør overholde enhver persons ret til at blive hørt, inden der træffes en individuel foranstaltning, som berører den pågældende negativt, og bør undgå overflødige udgifter og urimelige ulemper for de berørte personer.

Det forudsættes således i forordningens præambelbetragtning nr. 129, at tilsynsmyndighedens anvendelse af beføjelser skal være proportional, og at beføjelserne anvendes i overensstemmelse med bestemmelser om procesretssikkerhed.

Forordningen forholder sig – ligesom databeskyttelsesdirektivet – ikke direkte til spørgsmålet om, hvorvidt adgang til lokaler kan ske uden retskendelse, men betinger dog udtrykkeligt i artikel 58, stk. 1, litra f, at det sker *i overensstemmelse med retsplejeregler* i EU-retten eller medlemsstaternes nationale ret. Det fremgår desuden af præambelbetragtning

nr. 129, at hvad angår adgang til lokaler bør undersøgelsesbeføjelserne udøves i overensstemmelse med *specifikke krav i medlemsstaternes retspleje*, f.eks. krav om forudgående retskendelse.

Som anført ovenfor om gældende ret skal Datatilsynet ved gennemførelse af inspektioner i medfør af persondatalovens § 62 iagttage proportionalitetsprincippet og reglerne om fremgangsmåde ved gennemførelse af tvangsindgreb uden for strafferetsplejen i retssikkerhedsloven. Desuden har selvinkrimineringsforbuddet i retssikkerhedslovens § 10 – som bl.a. skal ses i lyset af artikel 50 i EU's Charter for Grundlæggende Rettigheder – betydning for tilsynets anvendelse af beføjelsen til at kræve oplysninger. For nærmere herom henvises til afsnit 5.11. om anmeldelse af brud på sikkerheden, artikel 33.

Samlet set må det på denne baggrund antages, at tilsynsmyndigheden også fremover vil skulle iagttage reglerne i retssikkerhedsloven i forbindelse med anvendelse af beføjelserne i forordningen.

7.8.4. Overvejelser

Forordningens artikel 58, stk. 1, litra e og f, må i vidt omfang anses for at være en videreførelse og præcisering af gældende ret. For så vidt angår beføjelsen om adgang til lokaler efter artikel 58, stk. 1, litra f, er der imidlertid tale om en udvidelse af tilsynenes muligheder for adgang til lokaler hos private, da forordningen ikke giver mulighed for at fastsætte bestemmelser om begrænsning af inspektionsbeføjelsen svarende til persondatalovens § 62, stk. 3, hvorefter Datatilsynets inspektionsbeføjelse i forhold til behandlinger, som foretages for private, er begrænset til de typer af behandlinger, som er undergivet et krav om forudgående tilladelse.

7.9. Aktivitetsrapport, artikel 59

7.9.1. Præsentation

Efter databeskyttelsesforordningens artikel 59 skal hver tilsynsmyndighed udarbejde en årlig rapport om sin virksomhed.

7.9.2. Gældende ret

Af artikel 28, stk. 5, i databeskyttelsesdirektivet fremgår det, at hver tilsynsmyndighed med regelmæssige mellemrum udarbejder en rapport om sin virksomhed. Denne rapport skal offentliggøres.

Direktivets artikel 28, stk. 5, er gennemført i dansk ret ved persondatalovens § 65, hvorefter Datatilsynet afgiver en årlig beretning om sin virksomhed til Folketinget. Beretningen skal offentliggøres. Tilsynet kan i øvrigt offentliggøre sine udtalelser. Bestemmelsen i § 30 finder tilsvarende anvendelse.

Henvisningen til § 30 indebærer, at Datatilsynet er berettiget – og efter omstændighederne også forpligtet til – at undlade at offentliggøre oplysninger fra sager, som tilsynet har behandlet, hvis offentlighedens interesse i at få oplysninger, findes at burde vige for afgørende hensyn til private eller offentlige interesser.

Datatilsynet afgiver i overensstemmelse hermed hvert år en beretning til Folketinget, der beskriver tilsynets arbejde på forskellige områder. Årsberetningen, der alene er udarbejdet på dansk, sendes ud til et antal faste modtagere hvert år, ligesom den gøres tilgængelig på tilsynets hjemmeside. Datatilsynets årsberetninger for årene 2000-2003 indeholder gengivelse af konkrete sager af principiel interesse. Fra og med 2004 er Datatilsynet begyndt løbende at offentliggøre sine udtalelser og afgørelser i sager af generel interesse på tilsynets hjemmeside.

7.9.3. Databeskyttelsesforordningen

Det følger af databeskyttelsesforordningens artikel 59, at hver tilsynsmyndighed udarbejder en årlig rapport om sin virksomhed, eventuelt med en liste over, hvilke typer overtrædelser der er blevet anmeldt, og hvilke typer foranstaltninger der er truffet i henhold til artikel 58, stk. 2. Disse rapporter fremsendes til det nationale parlament, regeringen og andre myndigheder, der er udpeget efter medlemsstaternes nationale ret. De gøres tilgængelige for offentligheden, Kommissionen og Databeskyttelsesrådet.

Kravet om, at den kommende tilsynsmyndighed skal udarbejde en årlig rapport om tilsynets virksomhed, svarer til den nuværende ordning med Datatilsynets årsberetning. Som noget nyt lægges der med forordningens artikel 59 op til, at der eventuelt orienteres om typer af overtrædelser og hvilke foranstaltninger, der er foretaget i den anledning.

Det fremgår ikke af forordningens artikel 59, hvilket sprog rapporten skal udarbejdes på. Når imidlertid henses til, at rapporten skal gøres tilgængelig for Kommissionen og Databeskyttelsesrådet, forudsætter det, at der som minimum udarbejdes et resume på engelsk.

7.9.4. Overvejelser

Kravet i forordningens artikel 59 om udarbejdelse af en årlig rapport om tilsynsmyndighedens virksomhed er ikke nyt. Indholdet kan dog fremover ende med at være en smule anderledes end Datatilsynets nuværende årsberetninger, idet der som nævnt ovenfor i forord-

ningen lægges op til, at der eventuelt orienteres om typer af overtrædelser, og hvilke foranstaltninger der er foretaget i den anledning. Endvidere udvides kredsen af modtagere af årsberetningen, idet den skal gøres tilgængelig også for Kommissionen og Databeskyttelsesrådet, hvilket må forventes at indebære, at der som minimum udarbejdes et resume på engelsk.

8. Forordningens kapitel VII: Samarbejde og sammenhæng

8.1. Samarbejde mellem tilsynsmyndigheder, artikel 60

8.1.1. Præsentation

I en meddelelse til Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget[798] fra 2010 udtalte Kommissionen, forud for sit forslag til databeskyttelsesforordning fra 2012[799], bl.a., at det er Kommissionens opfattelse, at databeskyttelsesmyndighederne bør intensivere deres indbyrdes samarbejde og koordinere deres arbejde bedre, ikke mindst når de står over for problemer, som i deres natur har en grænseoverskridende dimension. Ifølge Kommissionen er dette særligt tilfældet, når multinationale virksomheder har sæde i flere medlemsstater og opererer i hvert af disse lande.

Budskabet i Kommissionens meddelelse fra 2010 blev efterfølgende gentaget i Kommissionens oprindelige forslag til databeskyttelsesforordning fra 2012, hvor det, i de indledende bemærkninger til forslaget, bl.a. fremgår, at det nuværende databeskyttelsesdirektiv i sin ramme stadig er forsvarlig, hvad angår dens målsætninger og principper, men at den ikke har forhindret en fragmentering af den måde, hvorpå beskyttelsen af personoplysninger gennemføres i EU's forskellige medlemsstater. Samtidig fremgår det, at det derfor er på tide, at der opbygges en stærkere og mere sammenhængende ramme for databeskyttelse i EU, som følges op af en effektiv håndhævelse, der sikrer, at den digitale økonomi kan udvikle sig på tværs af det indre marked, giver fysiske personer kontrol over deres egne oplysninger og styrker retssikkerheden og den praktiske sikkerhed for erhvervsdrivende og offentlige myndigheder.

De ovenfor anførte synspunkter er også at finde – næsten ordret – i den vedtagne databeskyttelsesforordnings præambelbetragtning nr. 9, hvoraf det fremgår, at målsætningerne og principperne i databeskyttelsesdirektivet stadig er gyldige, men direktivet har ikke forhindret en fragmentering af gennemførelsen af databeskyttelse i Unionen, manglende retssikkerhed eller en udbredt offentlig opfattelse af, at der er betydelige risici for beskyttelsen af fysiske personer, navnlig i forbindelse med onlineaktivitet. Forskelle i niveauet for beskyttelsen af fysiske personers rettigheder og frihedsrettigheder, navnlig retten til beskyttelse af personoplysninger, i forbindelse med behandling af personoplysninger i medlemsstaterne, kan forhindre fri udveksling af personoplysninger i Unionen. Disse forskelle kan derfor udgøre en hindring for udøvelsen af en række økonomiske aktiviteter på EU-plan, virke

[798] Meddelelse fra Kommissionen til Europa-parlamentet, Rådet, Det økonomiske og sociale udvalg og regionsudvalget, En global metode til beskyttelse af personoplysninger i Den Europæiske Union (KOM (2010) 609 endelig), s. 18.
[799] Kommissionens forslag af 25. januar 2013 (KOM (2012) 11 endelig).

konkurrenceforvridende og hindre myndighederne i at varetage de opgaver, de er pålagt i medfør af EU-retten. En sådan forskel i beskyttelsesniveauet skyldes forskelle i gennemførelsen og anvendelsen af databeskyttelsesdirektivet.

Kommissionen har således utvivlsomt et stort ønske om, at databeskyttelsesforordningen vil blive anvendt effektivt og ensartet i hele EU.

Databeskyttelsesforordningens kapitel VII indeholder på den baggrund regler om samarbejde mellem tilsynsmyndighederne i EU. Reglerne foreskriver forskellige former for samarbejde, herunder regler om fælles beslutningstagen i visse sager, gensidig bistand og fælles aktiviteter, ligesom kapitlet indeholder regler om en såkaldt ”sammenhængsmekanisme”, som skal sikre en ensartet anvendelse af forordningen, og som betyder at Det Europæiske Databeskyttelsesråd (herefter Databeskyttelsesrådet) i visse tilfælde skal udstede vejledende udtalelser og i visse tilfælde træffe afgørelser, som er bindende for tilsynsmyndighederne.

Kapitel VII’s væsentligste nyskabelse i forhold til de gældende regler om tilsynsmyndighedernes kompetence er forordningens artikel 60 om fælles beslutningstagen i visse sager, den såkaldte ”one-stop-shop mekanisme”, som indebærer, at én tilsynsmyndighed ("den ledende tilsynsmyndighed"), der som udgangspunkt er tilsynsmyndigheden ved den dataansvarliges hovedvirksomhed, i visse grænseoverskridende sager vil være enekompetent til at træffe afgørelse i konkrete sager.

For en gennemgang af de øvrige regler om samarbejde i forordningens kapitel VII, afdeling 1 (artikel 61-62) henvises til afsnit 8.2. og for så vidt angår reglerne om den såkaldte ”sammenhængsmekanisme” i forordningens kapitel VII, afdeling 2, (artikel 63-67) til afsnit 8.3.

8.1.2. Gældende ret

I hverken databeskyttelsesdirektivet eller persondataloven findes der bestemmelser, som svarer til databeskyttelsesforordningens artikel 60.

8.1.3. Databeskyttelsesforordningen

8.1.3.1. Samarbejde mellem tilsynsmyndigheder (artikel 60, stk. 1)

Det følger af forordningens artikel 60, stk. 1, at den ledende tilsynsmyndighed samarbejder i henhold til denne artikel med de andre berørte tilsynsmyndigheder med henblik på at nå til enighed. Den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder skal udveksle alle relevante oplysninger med hinanden.

For nærmere om begrebet ”den ledende tilsynsmyndighed” henvises til artikel 56.

Ved begrebet ”en berørt tilsynsmyndighed” forstås ifølge forordningen artikel 4, nr. 22, 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.

På samme måde fremgår det af præambelbetragtning nr. 124, at den ledende tilsynsmyndighed bør samarbejde med de andre berørte myndigheder, fordi den dataansvarlige eller databehandleren har en etablering på deres medlemsstats område, fordi de registrerede, der har bopæl på deres område, er påvirket i væsentlig grad, eller fordi der er blevet indgivet en klage til dem. Også hvis en registreret, der ikke har bopæl i den medlemsstat, har indgivet en klage, bør den tilsynsmyndighed, til hvem klagen er indgivet, være en berørt tilsynsmyndighed.

Af præambelbetragtning nr. 125 fremgår endvidere, at den ledende tilsynsmyndighed bør have kompetence til at vedtage bindende afgørelser vedrørende foranstaltninger, der anvender de beføjelser, den er tillagt i overensstemmelse med denne forordning. Tilsynsmyndigheden bør i sin egenskab af ledende tilsynsmyndighed nøje inddrage og koordinere de berørte tilsynsmyndigheder i beslutningsprocessen. Hvis der træffes afgørelse om helt eller delvist at afvise den registreredes klage, bør denne afgørelse vedtages af den tilsynsmyndighed, til hvem klagen er indgivet.

Det er i øvrigt vigtigt at være opmærksom på, at forordningens artikel 60 – dvs. hele ”one-stop-shop”-mekanismen – ikke er begrænset til kun at finde anvendelse i forbindelse med behandlingen af konkrete klagesager. Forordningens artikel 60 gælder således i alle sager, hvor der skal træffes afgørelser, der involverer en privat dataansvarlig eller databehandler, og hvor der er tale om en grænseoverskridende behandling af personoplysninger, jf. artikel 4, nr. 23.[800] Det vil med andre ord sige, at f.eks. sager om udpegning af en databeskyttelsesrådgiver, afgørelser i forbindelse med høringer af tilsynsmyndigheden i anledning af en konsekvensanalyse efter artikel 35, godkendelse eller tilbagekaldelse af en certificering vil

[800] One-stop-shop mekanismen finder ikke anvendelse ved behandlinger foretaget af offentlige myndigheder baseret på artikel 6, stk. 1, litra c og e, jf. artikel 55, stk. 2.

også kunne tænkes at skulle behandles i overensstemmelse med "one-stop-shop"-mekanismen, således som den kommer til udtryk i forordningens artikel 60.

Det bemærkes, at mekanismen imidlertid ikke finder anvendelse på sager, hvor der ikke er en dataansvarlig eller databehandler etableret i EU, jf. herved forordningens artikel 56.[801]

8.1.3.2. Gensidig bistand og fælles aktiviteter (artikel 60, stk. 2)

Af forordningens artikel 60, stk. 2, følger, at den ledende tilsynsmyndighed til enhver tid kan anmode andre berørte tilsynsmyndigheder om at yde gensidig bistand i henhold til artikel 61 og kan gennemføre fælles aktiviteter i henhold til artikel 62, navnlig med henblik på at foretage undersøgelser eller overvåge gennemførelsen af en foranstaltning vedrørende en dataansvarlig eller en databehandler, der er etableret i en anden medlemsstat.

8.1.3.3. Udkast til afgørelse (artikel 60, stk. 3)

Det følger af forordningens artikel 60, stk. 3, *1. pkt.*, at hvis den ledende tilsynsmyndighed beslutter at undersøge en sag yderligere, skal den ledende tilsynsmyndighed straks underrette de andre berørte tilsynsmyndigheder om sagens relevante oplysninger.

Det må i øvrigt antages, at når det i bestemmelsen står anført, at underretningen skal ske straks, hænger det sammen med, at det er vigtigt, at det sker så tidligt som muligt, så de berørte myndigheder har tid til at sætte sig ind i sagen, også under hensyn til de forholdsvis korte tidsfrister, der er for at komme med indsigelse mod et udkast til afgørelse.

Det fremgår ikke af bestemmelsen, hvad der forstås ved "alle relevante oplysninger". Det må i hvert fald være de oplysninger, der er nødvendige for at kunne vurdere sagen. Hvis der blandt de andre berørte tilsynsmyndigheder er et ønske om yderligere oplysninger, må de naturligvis kunne rette henvendelse til den ledende tilsynsmyndighed og anmode herom.

Den ledende tilsynsmyndighed forelægger endvidere ifølge forordningens artikel 60, stk. 3, *2. pkt*, straks et udkast til afgørelse for de andre berørte tilsynsmyndigheder med henblik på deres udtalelse og tager behørigt hensyn til de berørte tilsynsmyndigheders synspunkter.

Af præambelbetragtning nr. 130 fremgår i den forbindelse også, at hvis den tilsynsmyndighed, til hvem en klage er indgivet, ikke er den ledende tilsynsmyndighed, bør den ledende tilsynsmyndighed samarbejde tæt med den tilsynsmyndighed, til hvem klagen er indgivet, i overensstemmelse med bestemmelserne om samarbejde og sammenhæng i denne forordning. I sådanne tilfælde bør den ledende tilsynsmyndighed, når den træffer foranstaltnin-

[801] Også Artikel 29-gruppens retningslinjer (WP 244) af 13. december 2016 om identificering af den ledende tilsynsmyndighed for en dataansvarlig eller databehandler.

ger, der skal have retsvirkning, herunder pålæggelse af administrative bøder, tage størst muligt hensyn til synspunkterne hos den tilsynsmyndighed, til hvem klagen er indgivet, og som fortsat bør være kompetent til at foretage undersøgelser på sin egen medlemsstats område i samråd med den ledende tilsynsmyndighed.

8.1.3.4. Procedure ved indsigelser (artikel 60, stk. 4)

Hvis en af de andre berørte tilsynsmyndigheder inden for fire uger efter at have modtaget et udkast til afgørelse fra den ledende tilsynsmyndighed i overensstemmelse med stk. 3, fremkommer med en relevant og begrundet 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.

Begrebet "en relevant og begrundet indsigelse" er defineret i forordningens artikel 4, nr. 24, hvoraf fremgår, at en indsigelse mod et udkast til afgørelse om, hvorvidt der foreligger en overtrædelse af forordningen, eller hvorvidt en planlagt foranstaltning i forbindelse med den dataansvarlige eller databehandleren overholder forordningen, 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.

For at samarbejdet skal fungere, er det på den ene side vigtigt, at de berørte tilsynsmyndigheder nøje overvejer deres indsigelser, og holder sig til relevante indsigelser og kommer med en begrundelse for den pågældende indsigelse. På den anden side, er det også vigtigt, at den ledende tilsynsmyndighed er åben over for en berørt tilsynsmyndigheds indsigelse.

For nærmere om den såkaldte "sammenhængsmekanisme" henvises til forordningens kapitel VII, afdeling 2, (artikel 63-67).

8.1.3.5. Tilsynsmyndigheden følger indsigelse (artikel 60, stk. 5)

Hvis den ledende tilsynsmyndighed har til hensigt at følge den relevante og begrundede indsigelse, skal den ifølge forordningens artikel 60, stk. 5, forelægge de andre berørte tilsynsmyndigheder et revideret udkast til afgørelse med henblik på deres udtalelse.

Det reviderede udkast til afgørelse er denne gang underlagt proceduren i stk. 4 inden for en frist på to uger.

8.1.3.6. Ingen indsigelser (artikel 60, stk. 6)
Hvis ingen af de berørte tilsynsmyndigheder har fremsat indsigelser imod udkastet til afgørelse fra den ledende tilsynsmyndighed inden for den periode, der fremgår af stk. 4 (fire uger) og stk. 5 (to uger), skal den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder efter forordningens artikel 60, stk. 6, anses for at være enige i det foreliggende udkast til afgørelse og er bundet af afgørelsen.

8.1.3.7. Hvordan skal afgørelsen meddeles (artikel 60, stk. 7)
Det fremgår herefter af forordningens artikel 60, stk. 7, at den ledende tilsynsmyndighed vedtager afgørelsen og meddeler den til den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering, alt efter omstændighederne.

Den ledende tilsynsmyndighed underretter endvidere de andre berørte tilsynsmyndigheder og Databeskyttelsesrådet om den pågældende afgørelse, herunder ved at give et resumé af de relevante faktiske omstændigheder og begrundelser.

Det er til gengæld den tilsynsmyndighed, der har modtaget en eventuel klage, der underretter klageren om afgørelsen.

8.1.3.8. Underretning ved afvisning (artikel 60, stk. 8)
Som en undtagelse til forordningens artikel 60, stk. 7, følger det af artikel 60, stk. 8, at i de tilfælde, hvor en klage ikke bliver imødekommet eller i det hele afvises, skal den tilsynsmyndighed, der har modtaget klagen, vedtage afgørelsen og meddele denne til klageren, ligesom denne tilsynsmyndighed skal underrette den dataansvarlige om afgørelsen.

8.1.3.9. Delvis afvisning (artikel 60, stk. 9)
I forordningens artikel 60, stk. 9, fastslås det, at i de tilfælde, hvor den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder er enige om at afslå eller afvise dele af en klage og at behandle andre dele af klagen, skal der vedtages separate afgørelser for hver af disse dele af klagen.

Den ledende tilsynsmyndighed vedtager afgørelsen for den del, der vedrører foranstaltninger over for den dataansvarlige, og meddeler dette til den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering på dens medlemsstats område og underretter klageren herom, mens den tilsynsmyndighed, der har modtaget klagen, skal vedtage den del af afgørelsen, der vedrører afslag eller afvisning af klagen, og underretter klageren herom og meddeler dette til den dataansvarlige eller databehandleren.

8.1.3.10. Den dataansvarliges foranstaltninger i forbindelse med afgørelsen (artikel 60, stk. 10)

Af forordningens artikel 60, stk. 10, følger, at den dataansvarlige eller databehandleren efter at være blevet underrettet om afgørelsen i stk. 7 og 9 af den ledende tilsynsmyndighed, skal træffe de nødvendige foranstaltninger til at sikre overholdelse af afgørelsen for så vidt angår behandlingsaktiviteter i forbindelse med alle vedkommendes etableringer i Unionen.

Den dataansvarlige eller databehandleren skal endvidere ifølge bestemmelsen underrette den ledende tilsynsmyndighed om de foranstaltninger, der er truffet for at overholde afgørelsen. Den ledende tilsynsmyndighed underretter herefter de andre berørte tilsynsmyndigheder om den dataansvarlig eller databehandlerens foranstaltninger i anledning af afgørelsen.

Der henvises endvidere til præambelbetragtning nr. 126, hvoraf det fremgår, at afgørelsen bør træffes i fællesskab af den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder og bør være rettet mod den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering samt være bindende for den dataansvarlige og databehandleren. Den dataansvarlige eller databehandleren bør træffe de nødvendige foranstaltninger til at sikre overholdelse af denne forordning samt gennemførelse af den afgørelse, som af den ledende tilsynsmyndighed meddeles den dataansvarlige eller databehandlerens hovedvirksomhed for så vidt angår behandlingsaktiviteter i Unionen.

8.1.3.11. Hasteprocedure (artikel 60, stk. 11)

Det fremgår af forordningens artikel 60, stk. 11, at hvis en berørt tilsynsmyndighed under ekstraordinære omstændigheder har grund til at mene, at det er nødvendigt at handle omgående for at beskytte registreredes interesser, finder hasteproceduren i artikel 66 anvendelse.

8.1.3.12. Elektronisk udveksling af oplysninger (artikel 60, stk. 12)

Det fremgår endelig af forordningens artikel 60, stk. 12, at den ledende tilsynsmyndighed og de andre berørte tilsynsmyndigheder udveksler oplysninger til brug for behandlingen i denne artikel elektronisk i et standardformat.

8.1.4. Overvejelser

Som nævnt ovenfor findes der hverken i databeskyttelsesdirektivet eller persondataloven bestemmelser, som svarer til databeskyttelsesforordningens artikel 60.

Selvom tilsynsmyndighederne allerede nu i et vist omfang – på frivillig basis – har samarbejdet om en ensartet anvendelse af databeskyttelsesdirektivet i enkeltsager, må forordningens regler om en one-stop-shop-mekanisme forventes at skabe en ny virkelighed for især tilsynsmyndighederne, men i et vist omfang også for danske virksomheder, der opererer i flere medlemsstater.

Dette skyldes bl.a., at der med databeskyttelsesforordningens artikel 60 fastsættes meget detaljerede regler for, hvordan visse grænseoverskridende sager i den private sektor fremover skal behandles. Der kan således med forordningens regler opstå situationer, hvor en dansk virksomhed, der opererer i flere medlemsstater – som følge af tvistbilæggelsesreglen i forordningens artikel 65 – kan blive underlagt en bindende afgørelse, som det danske datatilsyn ikke er enig i, men som tilsynet alligevel bliver nødt til at håndhæve over for virksomheden.

Tilsynsmyndighederne må på denne baggrund indstille sig på at skulle samarbejde om en ensartet anvendelse af forordningen, i markant flere sager, end det hidtil er sket på frivillig basis efter databeskyttelsesdirektivet – og selve samarbejdet kommer også til at foregå på en helt anden måde end i dag.

8.2. Gensidig bistand og fælles aktiviteter, artikel 61 og 62

8.2.1. Præsentation

Databeskyttelsesforordningens kapitel VII indeholder regler om samarbejde mellem tilsynsmyndighederne i EU. Reglerne foreskriver forskellige former for samarbejde, herunder regler om fælles beslutningstagen i visse sager, gensidig bistand og fælles operationer, ligesom kapitlet indeholder regler om en såkaldt ”sammenhængsmekanisme”, som skal sikre en ensartet anvendelse af forordningen, og som betyder, at Det Europæiske Databeskyttelsesråd i visse tilfælde skal udstede vejledende udtalelser samt i visse tilfælde træffe afgørelser, som er bindende for tilsynsmyndig-hederne.

I det følgende foretages en gennemgang af forordningens artikel 61 om den bistand de enkelte tilsynsmyndigheder gensidigt skal yde hinanden og artikel 62 om tilsynsmyndighedernes fælles aktiviteter. Det må i øvrigt antages, at begge bestemmelser, der er udtryk for et langt mere formaliseret og væsentligt udbygget samarbejde, end det som tilsynsmyndighederne allerede har i dag, ikke udtømmende gør op med, hvilke muligheder tilsynsmyndighederne har for at samarbejde fremover. Der kan således også tænkes andre måder for samarbejde på en mere frivillig basis.

8.2.2. Gældende ret

Af artikel 28, stk. 6, 1. afsnit, i databeskyttelsesdirektivet fremgår det, at den enkelte tilsynsmyndighed – uanset hvilken national lov der måtte gælde for den pågældende behandling – er kompetent til på sin medlemsstats område at udøve de beføjelser, der tillægges den i overensstemmelse med artikel 28, stk. 3. Det fremgår endvidere, at myndigheden kan blive anmodet om at udøve sine beføjelser af en myndighed i en anden medlemsstat.

Herudover fremgår det af artikel 28, stk. 6, 2. afsnit, at tilsynsmyndighederne samarbejder med hinanden i det omfang, det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle nyttige oplysninger.

Det er i direktivets præambelbetragtning nr. 64 endvidere anført at tilsynsmyndighederne i de enkelte medlemsstater skal yde hinanden bistand i forbindelse med varetagelsen af deres opgaver for at sikre, at beskyttelsesreglerne overholdes fuldt ud overalt i Den Europæiske Union.

Databeskyttelsesdirektivets artikel 28, stk. 6, er gennemført i dansk ret ved persondatalovens § 64.

Efter § 64, stk. 1, der bygger på artikel 28, stk. 6, 1. afsnit, kan Datatilsynet af egen drift eller efter anmodning fra en anden medlemsstat påse, at en behandling af oplysninger, som finder sted i Danmark, er lovlig, uanset at den pågældende behandling er undergivet en anden medlemsstats lovgivning. Bestemmelserne i § 59 (om påbud og forbud) og § 62 (om Datatilsynets adgang til oplysninger og lokaler) finder tilsvarende anvendelse.

Datatilsynet er således med andre ord kompetent til at påse, at en behandling, som er undergivet en anden medlemsstats lovgivning, er lovlig. Datatilsynet vil kunne afkræve oplysninger af en eventuel databehandler, som er etableret i Danmark, eller af en repræsentant for den dataansvarlige, som befinder sig i Danmark, jf. § 62, stk. 1. Tilsynet vil endvidere kunne udføre inspektioner (tilsyn) efter reglerne i § 62, stk. 3-4. Herudover har tilsynet kompetence til at realitetsbehandle og afgøre sagen efter den pågældende medlemsstats materielle lovgivning. Dette må forventes at ske på grundlag af oplysninger fra tilsynsmyndigheden i det pågældende medlemsland. Endelig kan Datatilsynet efter reglerne i lovens § 59 meddele påbud eller forbud til en databehandler eller repræsentant for den dataansvarlige, hvis disse befinder sig i Danmark.[802]

For så vidt angår tilsynsmyndighedens kompetence henvises i øvrigt til artikel 55-56.

[802] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 372.

Som det fremgår ovenfor forudsættes det i direktivets artikel 28, stk. 6, 2. afsnit, at tilsynsmyndighederne i medlemsstaterne samarbejder i det omfang, det er nødvendigt for at opfylde deres forpligtelser, navnlig ved at udveksle alle nyttige oplysninger.

Af Registerudvalgets betænkning nr. 1345, side 373, fremgår, at det således ikke kan udelukkes, at direktivet i nogle situationer medfører, at der skal videregives personoplysninger til tilsynsmyndighederne i de øvrige medlemsstater, enten i forbindelse med at disse andre myndigheder undersøger en behandling i deres land, som er undergivet dansk lovgivning, eller i forbindelse med, at Datatilsynet foretager en undersøgelse i Danmark af et forhold, som er undergivet den anden medlemsstats lovgivning. Efter straffelovens § 152 og §§ 152 c – 152 f, sammenholdt med forvaltningslovens §§ 27 og 28, er der grænser for, hvilke oplysninger der lovligt vil kunne videregives, idet visse oplysninger er undergivet tavshedspligt. Hvis Datatilsynet frit skal kunne videregive alle oplysninger i overensstemmelse med direktivets artikel 28, stk. 6, 2. afsnit, skal der efter udvalgets opfattelse således tilvejebringes en særskilt hjemmel hertil.

Der følger derfor nu af lovens § 64, stk. 2, at Datatilsynet kan videregive oplysninger til tilsynsmyndigheder i andre medlemsstater i det omfang, det er nødvendigt for at påse overholdelsen af bestemmelserne i denne lov eller af den pågældende medlemsstats databeskyttelseslovgivning.

Tilsynsmyndighederne samarbejder i dag også i regi af den såkaldte Artikel 29-gruppe.

Artikel 29-gruppen har i tidens løb udgivet en lang række henstillinger, udtalelser mv., der selv om de ikke er bindende, må antages at have haft en vis normerende effekt for de nationale tilsynsmyndigheder og må dermed antages at have medvirket til at øge graden af harmonisering af udmøntningen af direktivets regler i medlemsstaterne.

Der ses i øvrigt flere eksempler på, at tilsynsmyndighederne på frivillig basis i regi af Artikel 29-gruppen (eller undergrupper dertil) har samarbejdet om problemstillinger, der har haft grænseoverskridende elementer.

8.2.3. Databeskyttelsesforordningen

8.2.3.1. Gensidig bistand (*artikel 61)*

8.2.3.1.1. Udveksling af oplysninger (artikel 61, stk. 1)

Af forordningens artikel 61, stk. 1, 1. pkt., følger, at tilsynsmyndighederne udveksler relevante oplysninger og yder hinanden gensidig bistand med henblik på at gennemføre og anvende denne forordning på en ensartet måde og træffer foranstaltninger med henblik på et effektivt samarbejde med hinanden.

Det fremgår endvidere af bestemmelsens stk. 1. 2. pkt., at gensidig bistand navnlig omfatter anmodninger om oplysninger og tilsynsforanstaltninger, som f.eks. anmodninger om gennemførelse af forudgående godkendelser og høringer, inspektioner og undersøgelser.

Af præambelbetragtning nr. 123 fremgår endvidere, at tilsynsmyndighederne bør føre tilsyn med anvendelsen af bestemmelserne i henhold til denne forordning og bidrage til ensartet anvendelse heraf i hele Unionen for at beskytte fysiske personer i forbindelse med behandling af deres personoplysninger og lette fri udveksling af personoplysninger på det indre marked. Til det formål bør tilsynsmyndighederne samarbejde med hinanden og Kommissionen, uden at der er behov for en aftale mellem medlemsstater om gensidig bistand eller om et sådant samarbejde.

Herudover fremgår det af præambelbetragtning nr. 133, at tilsynsmyndighederne bør bistå hinanden i forbindelse med udførelsen af deres opgaver og yde gensidig bistand for at sikre ensartet anvendelse og håndhævelse af forordningen på det indre marked.

Bestemmelsen vil kunne få stor betydning i forhold til de grænseoverskridende sager, men som det fremgår, er den efter sin ordlyd ikke begrænset til kun at finde anvendelse i sådanne tilfælde. Det er, som forordningens artikel 61 er formuleret, heller ikke et krav, at der er tale om gensidig bistand i forbindelse med en konkret undersøgelse eller en klagesag hos den anmodende tilsynsmyndighed, og bestemmelsen vil derfor i princippet også kunne benyttes til f.eks. af generel interesse at indhente oplysninger om den anmodede tilsynsmyndigheds praksis på et givent område. Sådanne generelle anmodninger bør imidlertid ikke behandles efter proceduren i artikel 61, men i stedet håndteres på en mere uformel måde af de involverede tilsynsmyndigheder.

Forordningens artikel 61 udelukker ikke mere uformelle samarbejder tilsynsmyndighederne imellem. Det må således med andre ord antages, at det fremover også vil være muligt for tilsynsmyndighederne at samarbejde på andre måder på frivillig basis, jf. i den forbindelse også forordningens artikel 57, stk. 1, litra g, hvorefter en af tilsynsmyndighedernes opgaver er at samarbejde med andre tilsynsmyndigheder om anvendelsen af denne forordning, *herunder* gennem udveksling af oplysninger og gensidig bistand, med henblik på at sikre ensartet anvendelse og håndhævelse af denne forordning. Der henvises endvidere til præambelbetragtning nr. 123, jf. ovenfor.

8.2.3.1.2. Besvarelse af anmodninger om bistand (artikel 61, stk. 2)

Ifølge forordningens artikel 61, stk. 2, træffer hver tilsynsmyndighed alle passende foranstaltninger, som er nødvendige for at besvare en anmodning fra en anden tilsynsmyndighed uden unødig forsinkelse og senest en måned efter modtagelsen af anmodningen. Sådanne

foranstaltninger kan bl.a. omfatte videregivelse af relevante oplysninger om gennemførelsen af en undersøgelse.

Den tilsynsmyndighed, der modtager anmodningen om gensidig bistand har således en absolut frist på en måned til at svare, men selv inden for denne frist, skal de svare uden unødig forsinkelse, hvilket vil sige hurtigst muligt.

8.2.3.1.3. Krav til anmodningen (artikel 61, stk. 3)
For så vidt angår krav til anmodningen om bistand fremgår det af forordningens artikel 61, stk. 3, at anmodninger om bistand skal indeholde alle nødvendige oplysninger, herunder formålet med og grunden til anmodningen. Udvekslede oplysninger må kun anvendes til det formål, som er angivet i anmodningen.

På denne måde sikres det, at de anmodninger, der sendes, er velovervejede, ligesom det også gerne skulle gøre det lettere for den tilsynsmyndighed, der modtager anmodningen at forholde sig til anmodningen og komme med et anvendeligt svar.

Det forventes i øvrigt, at tilsynsmyndighederne i regi af Artikel 29-gruppen bl.a. vil udarbejde en formular, der vil kunne benyttes til anmodninger om gensidig bistand med det formål at sikre, at anmodningen indeholder alle nødvendige oplysninger.

8.2.3.1.4. Krav om svar (artikel 61, stk. 4)
Det fremgår af forordningens artikel 61, stk. 4, at den anmodede tilsynsmyndighed ikke må afvise at imødekomme anmodningen, medmindre den ikke har kompetence med hensyn til genstanden for anmodningen eller de foranstaltninger, som den anmodes om at iværksætte (litra a), eller imødekommelse af anmodningen ville udgøre en overtrædelse af denne forordning eller af EU-ret eller medlemsstaternes nationale ret, som den tilsynsmyndighed, der modtager anmodningen, er underlagt (litra b).

Udgangspunktet efter bestemmelsen er, at en tilsynsmyndighed, der har modtaget en anmodning om gensidig bistand, *ikke* må afvise at imødekomme anmodningen. Der er således kun i de to forholdsvis begrænsede tilfælde, der er opregnet i bestemmelsen, at den anmodede tilsynsmyndighed kan undlade at besvare anmodningen. Der vil dog stadig skulle gives et svar om, at man ikke kan svare, og med en begrundelse herfor. Se nærmere nedenfor.

Det bemærkes i den forbindelse, at det fremgår af forordningens artikel 64, stk. 2, at en tilsynsmyndighed, formanden for Databeskyttelsesrådet eller Kommissionen kan kræve, at ethvert almengyldigt spørgsmål, der har virkninger i mere end én medlemsstat, drøftes af

Databeskyttelsesrådet med henblik på en udtalelse, navnlig hvis en kompetent tilsynsmyndighed ikke opfylder forpligtelserne vedrørende gensidig bistand, jf. artikel 61, eller vedrørende fælles aktiviteter, jf. artikel 62.

Selvom ovennævnte bestemmelse i relation til forordningens artikel 61 og artikel 62 må antages navnlig at være møntet på de tilsynsmyndigheder, som f.eks. ikke sender et svar på en anmodning eller konsekvent gør det efter fristen er udløbet, så må det omvendt også være muligt i medfør af denne bestemmelse at "indbringe" en tilsynsmyndighed, der vælger gentagne gange at gøre brug af artikel 61 og artikel 62 i situationer, hvor vurderingen er, at det ikke var nødvendigt, idet anmodningerne f.eks. har været meget lidt underbygget.

For nærmere om den såkaldte "sammenhængsmekanisme", herunder Databeskyttelsesrådet, henvises til 63-67 samt artikel 68-76.

8.2.3.1.5. Svar på anmodningen (artikel 61, stk. 5)
Af forordningens artikel 61, stk. 5, fremgår det, at den anmodede tilsynsmyndighed underretter den anmodende tilsynsmyndighed om resultaterne eller efter omstændighederne om fremskridtene med de foranstaltninger, der er truffet for at imødekomme anmodningen. Den anmodede tilsynsmyndighed begrunder endvidere enhver afvisning af at imødekomme en anmodning i henhold til stk. 4.

Der henvises i øvrigt til det ovenfor anførte om muligheden for at "indbringe" en tilsynsmyndighed for Databeskyttelsesrådet, hvis det vurderes, at tilsynsmyndigheden ikke opfylder forpligtelserne vedrørende gensidig bistand, jf. artikel 61, eller vedrørende fælles aktiviteter, jf. artikel 62.

8.2.3.1.6. Elektronisk svar (artikel 61, stk. 6)
I forordningens artikel 61, stk. 6, fastslås det, at den anmodede tilsynsmyndighed som hovedregel fremsender de oplysninger, som andre tilsynsmyndigheder anmoder om, elektronisk i et standardformat.

Hovedreglen er således, at der skal anvendes elektronisk kommunikation. Der skal derfor opnås enighed om, hvilket standardformat, der skal ske udveksling i.

8.2.3.1.7. Betaling (artikel 61, stk. 7)
Det fremgår af forordningens artikel 61, stk. 7, at tilsynsmyndigheder, der anmodes om bistand, ikke må opkræve gebyr for foranstaltninger, der træffes af dem på grundlag af en anmodning om gensidig bistand. Tilsynsmyndighederne kan vedtage regler om at godtgøre

hinanden for specifikke udgifter, der opstår under ekstraordinære omstændigheder, når der ydes gensidig bistand.

For at der ikke skal opstå spørgsmål om betaling i alt for mange situationer, vil det i øvrigt være praktisk, hvis tilsynsmyndighederne kunne blive enige om, at der med udtrykket "ekstraordinære omstændigheder" sigtes til ikke helt ubetydelige udgifter, som begge parter indvilger i er nødvendige at afholde, og at der i forbindelse med anmodninger om bistand, hvor det allerede fra starten af er klart, at sådanne udgifter kan forekomme, udfærdiges konkrete aftaler herom, inden udgifterne afholdes.

8.2.3.1.8. Foreløbige foranstaltninger (artikel 61, stk. 8)
Hvis en tilsynsmyndighed ikke giver de oplysninger, der er omhandlet i artikel 61, stk. 5, inden for en måned efter modtagelsen af en anmodning fra en anden tilsynsmyndighed, kan den anmodende tilsynsmyndighed ifølge forordningens artikel 61, stk. 8, 1. pkt., vedtage en foreløbig foranstaltning på sin medlemsstats område i henhold til artikel 55, stk. 1. Endvidere fremgår det af artikel 61, stk. 8, 2. pkt., at i dette tilfælde antages kravet om behovet for at handle omgående, jf. artikel 66, stk. 1, at være opfyldt, og at kræve en hurtig bindende afgørelse fra Databeskyttelsesrådet, jf. artikel 66, stk. 2.

Om bestemmelsen fremgår det endvidere af præambelbetragtning nr. 133, at en tilsynsmyndighed, der har anmodet om gensidig bistand, kan vedtage en foreløbig foranstaltning, hvis myndigheden ikke har modtaget svar på en anmodning om gensidig bistand inden for en måned fra den anden tilsynsmyndigheds modtagelse af anmodningen.

Om hasteproceduren i forordningens artikel 66 henvises i øvrigt til artikel 63-67 og artikel 68-76.

8.2.3.1.9. Gennemførelsesretsakter for format og procedurer (artikel 61, stk. 9)
Kommissionen kan ifølge forordningens artikel 61, stk. 9, 1. pkt., ved gennemførelsesretsakter fastlægge format og procedurer for gensidig bistand som omhandlet i denne artikel og ordninger for elektronisk udveksling af oplysninger mellem tilsynsmyndigheder og mellem tilsynsmyndigheder og Databeskyttelsesrådet, navnlig standardformatet omhandlet i artikel 61, stk. 6.

Hvis Kommissionen benytter muligheder for gennemførelsesretsakter, skal disse ifølge artikel 61, stk. 9, 2. pkt., vedtages efter undersøgelsesproceduren i artikel 92, stk. 2.

8.2.3.2. Tilsynsmyndighedernes fælles aktiviteter

8.2.3.2.1. Fælles aktiviteter (artikel 62, stk.1)

Det fremgår af forordningens artikel 62, stk. 1, at hvis det er hensigtsmæssigt, gennemfører tilsynsmyndighederne fælles aktiviteter, herunder fælles undersøgelses- og håndhævelsesforanstaltninger, som medlemmer eller medarbejdere fra andre medlemsstaters tilsynsmyndigheder deltager i.

Af præambelbetragtning nr. 134 fremgår endvidere, at hver tilsynsmyndighed, hvis det er relevant, bør deltage i fælles aktiviteter sammen med andre tilsynsmyndigheder. En tilsynsmyndighed, der modtager en anmodning, bør være forpligtet til at besvare anmodningen inden for en angiven frist.

Med udtrykket "fælles aktiviteter" sigtes bl.a. til alt fra udarbejdelse af fælles vejledninger og andet informationsmateriale om forskellige emner i forordningen til fælles inspektioner (tilsynsbesøg) og håndhævelsesindsatser.

8.2.3.2.2. Deltagerne (artikel 62, stk. 2)

Af forordningens artikel 62, stk. 2, 1. pkt., fremgår det, at hvis den dataansvarlige eller databehandleren har etableringer i flere medlemsstater, eller hvor et betydeligt antal registrerede i mere end én medlemsstat sandsynligvis påvirkes i væsentlig grad af behandlingsaktiviteter, har tilsynsmyndigheden i hver af disse medlemsstater ret til at deltage i fælles aktiviteter.

Det fremgår endvidere af forordningens artikel 62, stk. 2, 2. pkt., at initiativet til at indbyde disse ovennævnte tilsynsmyndigheder til at deltage i fælles aktiviteter skal komme fra den tilsynsmyndighed, der er kompetent i henhold til artikel 56, stk. 1 eller 4. Det vil sige den ledende tilsynsmyndighed, som i øvrigt straks skal besvare en tilsynsmyndigheds anmodning om deltagelse.

Det bemærkes, at det naturligvis også er muligt for den ledende tilsynsmyndighed, der tager initiativ til fælles aktiviteter, at invitere andre tilsynsmyndigheder end de ovennævnte "særlige" tilsynsmyndigheder til at deltage. Forordningens artikel 62, stk. 2, fastslår således blot, hvem der skal inviteres med. Det må endvidere antages, at det er muligt for en tilsynsmyndighed selv, at anmode om at kunne deltage i en sådan fælles aktivitet. Den ledende tilsynsmyndighed må så tage stilling til en sådan eventuel anmodning.

Ordlydsmæssigt svarer indholdet af bestemmelsen i øvrigt til definitionen af, hvornår der er tale om en grænseoverskridende behandling, ligesom de tilsynsmyndigheder, der har ret til at deltage, stort set svarer til definitionen af, hvornår man er en såkaldt "berørt" tilsyns-

myndighed. Forskellen ligger i, at man i dette tilfælde ikke har krav på at blive inviteret til en fælles aktivitet, hvis man som tilsynsmyndighed blot har modtaget en klage fra en registreret, som det er tilfældet ved afgørelser af sager efter artikel 60.

8.2.3.2.3. Delegation af beføjelser (artikel 62, stk. 3)

Ifølge forordningens artikel 62, stk. 3, 1. pkt., kan en tilsynsmyndighed i overensstemmelse med medlemsstatens nationale ret og med den udsendende tilsynsmyndigheds godkendelse delegere beføjelser, herunder undersøgelsesbeføjelser, til den udsendende tilsynsmyndigheds medlemmer eller medarbejdere, som deltager i fælles aktiviteter, eller, for så vidt national ret i værtstilsynsmyndighedens medlemsstat tillader det, tillade, at den udsendende tilsynsmyndigheds medlemmer eller medarbejdere udøver deres undersøgelsesbeføjelser i overensstemmelse med retten i den udsendende tilsynsmyndigheds medlemsstat.

Det fastslås endvidere i forordningens artikel 62, stk. 3, 2. pkt., at sådanne undersøgelsesbeføjelser kun må udøves under vejledning og i tilstedeværelse af værtstilsynsmyndighedens medlemmer eller medarbejdere, ligesom den udsendende tilsynsmyndigheds medlemmer eller medarbejdere er underlagt national ret i værtstilsynsmyndighedens medlemsstat.

Bestemmelsen indebærer med andre ord, at den såkaldte værtstilsynsmyndighed – i overensstemmelse med sin nationale lovgivning og med den udsendende tilsynsmyndigheds godkendelse – kan træffe beslutning om at overføre sine beføjelser, herunder undersøgelsesbeføjelser, til medlemmer eller personale fra den udsendende tilsynsmyndighed. For så vidt værtstilsynsmyndighedens lovgivning giver mulighed herfor, kan værtsmyndigheden endvidere tillade, at den udsendende tilsynsmyndigheds medlemmer eller medarbejdere udøver deres forvaltningsbeføjelser i overensstemmelse med den udsendende tilsynsmyndigheds lovgivning.

Hvis f.eks. lovgivningen i Frankrig tillader dette, kan tilsynsmyndigheden i Frankrig, f.eks. overlade det til tilsynsmyndigheden i Italien at udtale kritik over for en dataansvarlig, der er etableret i Frankrig i forbindelse med en sag, der er under behandling i såvel Frankrig og Italien som en fælles aktivitet i regi af artikel 62, hvis den italienske tilsynsmyndighed ellers kan acceptere dette. Tilsynsmyndigheden i Frankrig kan endvidere lade delegationen gå så vidt til også f.eks. at omfatte retten til at kræve alle oplysninger af den pågældende fransk etablerede dataansvarlige. Den italienske tilsynsmyndigheds beføjelser vil i begge de nævnte situationer svare til de beføjelser, som tilsynsmyndigheden i Frankrig er tildelt.
Det kan imidlertid også forholde sig således, at det er i overensstemmelse med lovgivningen i Frankrig, at tilsynsmyndighed i Italien udøver sine egne undersøgelsesbeføjelser i overensstemmelse med, hvad der følger af italiensk lovgivning. I sidstnævnte tilfælde må

den italienske tilsynsmyndigheds undersøgelsesbeføjelser imidlertid kun udøves under vejledning og i tilstedeværelse af den franske tilsynsmyndigheds medlemmer eller medarbejdere, ligesom det italienske tilsynsmyndigheds medlemmer eller medarbejdere er underlagt fransk lovgivning.

I forhold til rammerne for sådanne beføjelser i dansk ret anses danske myndigheder som udgangspunkt for at være enekompetente til at udøve myndighedsbeføjelser inden for det danske territorium. Myndighedsudøvelse er således en (ene)beføjelse, der tilkommer rigets myndigheder. Et samarbejde med udenlandske myndigheder, der bliver udført under dansk ledelse, og hvor udenlandske embedsmænd ikke får adgang til på egen hånd at udøve beføjelser på dansk territorium, vil dog som udgangspunkt ikke rejse spørgsmål i forhold til grundloven. Der henvises i den forbindelse til punkt 2.6 i de almindelige bemærkninger til lov nr. 479 af 17. juni 2008, der gennemførte den såkaldte prümafgørelse i dansk ret, jf. lovforslag nr. L 77 af 27. februar 2008.

Danske myndigheder vil således ikke kunne delegere til udenlandske myndigheder at udøve beføjelser på dansk territorium på egen hånd. Det vil derfor ikke være i overensstemmelse med national ret at delegere beføjelser, herunder undersøgelsesbeføjelser, til den udsendende tilsynsmyndigheds medlemmer eller medarbejdere eller at tillade den udsendende tilsynsmyndighed at udøve undersøgelsesbeføjelser i overensstemmelse med retten i den udsendende tilsynsmyndigheds medlemsstat. Dansk ret vil derimod ikke være til hinder for, at en udenlandsk tilsynsmyndigheds medlemmer eller medarbejdere gives ret til at være til stede under den danske tilsynsmyndigheds udøvelse af myndighed på dansk territorium.

8.2.3.2.4. Erstatningsansvar (artikel 62, stk. 4-6)

Forordningens artikel 62, stk. 4-6, indeholder regler om ansvarsfordeling og lovvalg i forbindelse med erstatning for eventuelle skader, som opstår i forbindelse med udførelse af de fælles aktiviteter.

Af forordningens artikel 62, stk. 4, følger således, at hvis en udsendende tilsynsmyndigheds medarbejdere i henhold til artikel 62, stk. 1, udfører aktiviteter i en anden medlemsstat, påtager værtstilsynsmyndighedens medlemsstat sig ansvaret for deres handlinger, herunder erstatningsansvar for enhver skade, som de måtte forvolde under udførelsen af deres aktiviteter, i overensstemmelse med retten i den medlemsstat, på hvis område de udfører aktiviteter.

Endvidere fremgår det af forordningens artikel 62, stk. 5, at den medlemsstat, på hvis område skade forvoldes, erstatter den pågældende skade på samme betingelser som skader

forvoldt af dens egne medarbejdere. Den udsendende tilsynsmyndigheds medlemsstat, hvis medarbejdere har forvoldt skade på personer på en anden medlemsstats område, skal fuldt ud godtgøre alle beløb, som denne anden medlemsstat har betalt i skadeserstatning til de berettigede personer på deres vegne.

Det fremgår endvidere af forordningens artikel 62, stk. 6, at uden at det berører udøvelsen af rettigheder over for tredjemand og med undtagelse af det i artikel 62, stk. 5, omhandlede tilfælde, giver den enkelte medlemsstat i det tilfælde, der er omhandlet i artikel 62, stk. 1, afkald på at kræve godtgørelse fra en anden medlemsstat i forbindelse med skade som omhandlet i artikel 62, stk. 4.

8.2.3.2.5. Foreløbige foranstaltninger (artikel 61, stk. 7)

Det fremgår af forordningens artikel 62, stk. 7, 1. pkt., at hvis der planlægges en fælles aktivitet, og en tilsynsmyndighed ikke opfylder forpligtelsen i artikel 62, stk. 2, 2. pkt., inden for en måned, kan de andre tilsynsmyndigheder vedtage en foreløbig foranstaltning på deres medlemsstats område i overensstemmelse med artikel 55.

Endvidere fremgår det af artikel 62, stk. 7, 2. pkt., at kravet om behovet for at handle omgående, jf. artikel 66, stk. 1, i dette tilfælde antages at være opfyldt, ligesom der er adgang til at kræve en hurtig bindende afgørelse fra Databeskyttelsesrådet, jf. artikel 66, stk. 2.

8.2.4. Overvejelser

Hvor databeskyttelsesforordningens artikel 62 må anses for en nyskabelse i forhold til databeskyttelsesdirektivet, så svarer forordningens artikel 61 formelt set til direktivets artikel 28, stk. 6. Tilsynsmyndighederne er således allerede i dag efter direktivet forpligtet til at samarbejde med hinanden, herunder udveksle relevante oplysninger og yde hinanden gensidig bistand. Det nye i forhold til begge disse bestemmelser i forordningen er imidlertid, at samarbejdet i vidt omfang ændrer karakter fra at være noget, der indtil nu er foregået ganske uformelt, til fremover at blive meget mere formaliseret. Der har f.eks. ikke tidligere været fastsat en pligt for den anmodede tilsynsmyndighed til at svare indenfor en given frist, ligesom tilsynsmyndighederne i dag heller ikke har mulighed for at "indbringe" hinanden for Artikel-29-gruppen i tilfælde af, at en tilsynsmyndighed efter en anden tilsynsmyndigheds opfattelse ikke lever op til sine forpligtelser til at samarbejde.

Der er næppe nogen tvivl om, at begge bestemmelser vil indebære, at nogle tilsynsmyndigheder, herunder også Datatilsynet, vil være nødt til at engagere sig yderligere i samarbejdet med andre tilsynsmyndigheder i henhold til forordningens artikel 61 og artikel 62.

Det må i øvrigt – som tidligere anført – antages, at forordningens artikel 61 og 62 ikke udtømmende gør op med, hvilke muligheder, der er for at samarbejde. Det vil også være muligt at samarbejde på andre måder på frivillig basis.

8.3. Sammenhæng, artikel 63-67

8.3.1. Præsentation

Af Kommissionens forslag fra 2012 fremgår det, at der forud for forslaget var blevet gennemført målrettede høringer af centrale aktører, ligesom der var blevet afholdt målrettede workshopper og seminarer om specifikke spørgsmål. I forbindelse med disse høringer mv. var den nuværende fragmentering af beskyttelsen af personoplysninger i EU blevet skarpt kritiseret af navnlig økonomiske aktører, der ønsker øget retssikkerhed og harmonisering af reglerne om beskyttelse af personoplysninger.

Kommissionen har således utvivlsomt et stort ønske om, at databeskyttelsesforordningen vil blive anvendt effektivt og ensartet i hele EU.

Den ønskede harmonisering er imidlertid vanskelig at opnå i praksis, hvis ikke tilsynsmyndighederne (og til dels også Kommissionen selv) samarbejder herom. Det må antages at være i erkendelse heraf, at man i databeskyttelsesforordningens kapitel VII, afdeling 2 om sammenhæng (artikel 63-67) har fastsat meget deltaljerede regler for, hvordan tilsynsmyndighederne skal samarbejde med hinanden om en ensartet anvendelse af forordningen.

Kapitlet om sammenhæng er opbygget således, at der med databeskyttelsesforordningens artikel 63 fastsættes en sammenhængsmekanisme, der som en slags principerklæring fastslår, at tilsynsmyndighederne skal samarbejde med hinanden, og hvor det er relevant med Kommissionen, med henblik på en ensartet anvendelse af databeskyttelsesforordningen i hele EU.

Reglerne i databeskyttelsesforordningens artikel 64-67 – som udgør de øvrige bestemmelser i sammenhængskapitlet – skal herefter anvendes for at få sammenhængsmekanismen i artikel 63 til at fungere i praksis.

Der henvises endvidere til afsnit 8.1. og 8.2. om reglerne om samarbejde i databeskyttelsesforordningens kapitel VII, afdeling 1 (artikel 60-62), da disse regler også vil få stor betydning for, om det lykkes at opnå en ensartet anvendelse af forordningen i hele EU.

8.3.2. Gældende ret

I hverken databeskyttelsesdirektivet eller persondataloven findes der bestemmelser, som svarer til databeskyttelsesforordningens artikel 63-67.

Det tætteste man i de nuværende regler kommer på en bestemmelse, der skal medvirke til at sikre en ensartet anvendelse af databeskyttelsesdirektivet er direktivets artikel 30, stk. 2. Af denne bestemmelse fremgår det, at hvis Artikel 29-gruppen konstaterer forskelle mellem medlemsstaternes lovgivning eller praksis, der kan være til fare for en ensartet beskyttelse af personer i forbindelse med behandling af personoplysninger inden for Fællesskabet, skal gruppen underrette Kommissionen derom. Bestemmelsen i artikel 30, stk. 2, er umiddelbart af meget overordnet karakter og fastsætter ikke nærmere regler for, hvordan tilsynsmyndighederne skal samarbejde om en ensartet anvendelse af direktivet. I stedet overlades det til Kommissionen at forsøge at løse eventuelle problemer, hvilket kan være svært, med mindre medlemsstaternes nationale regler og praksis decideret er i strid med direktivet.

Herudover fremgår det af databeskyttelsesdirektivets artikel 28, stk. 6, at tilsynsmyndighederne skal samarbejde med hinanden i det omfang, det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle nyttige oplysninger. Formålet med denne bestemmelse er imidlertid, at medlemsstaterne i et eller andet omfang skal samarbejde med hinanden for at sikre, at bestemmelserne i de nationale lovgivninger, som vedtages til gennemførelse af direktivet, overholdes, uanset hvor behandlingen finder sted.[803] Formålet er således ikke at sikre en ensartet anvendelse af direktivet.

Selvom databeskyttelsesdirektivet ikke indeholder nærmere regler om tilsynsmyndighedernes samarbejde om en ensartet anvendelse af direktivet, betyder dette dog ikke, at medlemsstaterne ikke i et vist omfang samarbejder derom.

Der har således i Artikel 29-gruppens levetid været flere eksempler på, at medlemsstaterne har samarbejdet om problemstillinger, der har et grænseoverskridende element.

Som et nyere eksempel på samarbejde mellem tilsynsmyndighederne kan der peges på tilsynsmyndighedernes samarbejde i forlængelse af EU-Domstolens dom af 6. oktober 2015 i sag C-362/14 (Maximillian Schrems mod det irske datatilsyn). Dommen er nærmere omtalt i afsnit 6.2. om databeskyttelsesforordningens artikel 45.

[803] Se Registerudvalgets betænkning nr. 1345/ 1997, afsnit 3.9.4.7.

Med dommen fastslog EU-Domstolen, at den såkaldte Safe Harbor-ordning[804], hvorefter europæiske dataeksportører havde kunnet overføre personoplysninger til visse dataimportører (virksomheder m.fl.) i USA, var ugyldig.

Efter dommen udtalte Artikel 29-gruppen bl.a., at det var nødvendigt, at de europæiske datatilsyn havde en fælles tilgang til implementeringen af dommen fra EU-Domstolen, og at gruppen bl.a. derfor ville analysere konsekvenserne af dommen i relation til de øvrige overførselsgrundlag, herunder Kommissionens standardkontrakter og Binding Corporate Rules.

Dette meget omfattende analysearbejde foregik i flere undergrupper til Artikel 29-gruppen og mundede ud i en række udtalelser bl.a. i forbindelse med den senere vedtagelse af det såkaldte EU-U.S. Privacy Shield, som afløser føromtalte Safe Harbor-ordning.[805]

Et andet nyere eksempel på samarbejde er tilsynsmyndighedernes samarbejde i forlængelse af, at WhatsApp i august 2016 ændrede deres brugervilkår således, at WhatsApp fremover vil dele brugerinformationer inden for "Facebook familien", herunder bl.a. til markedsførings- og reklameformål.

Problemstillingen i WhatsApp-sagen var bl.a., at behandling af brugerinformationer til markedsførings- og reklameformål ikke var en del af WhatsApps brugervilkår, da de eksisterende brugere oprettede en brugerkonto hos WhatsApp. Hertil kommer, at de nye vilkår syntes at være i modstrid med tidligere udtalelser fra WhatsApp og Facebook om, at der aldrig ville blive udvekslet oplysninger imellem selskaberne.

Idet de ændrede brugervilkår ville berøre mange borgere i hele EU, valgte Artikel 29-gruppen efterfølgende i oktober 2016 skriftligt at rette henvendelse til WhatsApp med henblik på afklaring af en række bekymringer i forhold til de nye brugervilkår, herunder i forhold til gyldigheden af brugernes samtykker mv.

Med hensyn til spørgsmålet om en ensartet anvendelse af direktivet skrev Artikel 29-gruppen bl.a. følgende i sit brev til WhatsApp:

> "Therefore, the members of the Working Party 29 will act in a coordinated way and take actions according to their respective competences and powers in order to clarify these points of concern and to ensure that the principles and rights set forth in Euro-

[804] Kommissionens beslutning 2000/520/EF.
[805] Se Artikel 29-gruppens udtalelse af 13. april 2016 om EU-U.S. Privacy Shield (WP 238).

pean and national Data Protection laws are upheld in a consistent manner across the EU."

Fælles for tilsynsmyndighedernes samarbejde i ovennævnte sager – samt i andre lignende sager – er, at samarbejdet er frivilligt, men at tilsynsmyndighederne konkret har fundet det formålstjenstligt at samarbejde grundet sagernes grænseoverskridende karakter.

8.3.3. Databeskyttelsesforordningen

8.3.3.1. Sammenhængsmekanisme (artikel 63)

Det følger af databeskyttelsesforordningens artikel 63, at tilsynsmyndighederne skal samarbejde med hinanden, og, hvis det er relevant med Kommissionen, med henblik på at bidrage til en ensartet anvendelse af databeskyttelsesforordningen i hele Unionen gennem den sammenhængsmekanisme, der er omhandlet i denne afdeling (kapitel VII, afdeling 2 om sammenhæng).

Af præambelbetragtning nr. 135 fremgår det, at sammenhængsmekanismen for samarbejde mellem tilsynsmyndighederne bør etableres for at sikre ensartet anvendelse af databeskyttelsesforordningen i hele Unionen. Det fremgår endvidere, at mekanismen navnlig bør anvendes, når en tilsynsmyndighed agter at vedtage en foranstaltning, der skal have retsvirkning, i forhold til behandlingsaktiviteter, der i væsentlig grad påvirker et betydeligt antal registrerede i flere medlemsstater. Endvidere fremgår det, at mekanismen også bør anvendes, hvis en berørt tilsynsmyndighed eller Kommissionen ønsker, at en sådan sag behandles inden for sammenhængsmekanismen. Det fremgår endelig, at mekanismen ikke berører foranstaltninger, som Kommissionen måtte træffe som led i udøvelsen af sine beføjelser i henhold til traktaterne (f.eks. traktatskrænkelsessager som følge af manglende overholdelse af forordningen).

Herudover fremgår det af præambelbetragtning nr. 138, at anvendelse af sammenhængsmekanismen bør være en betingelse for lovligheden af en af en tilsynsmyndighed truffet foranstaltning, der skal have retsvirkning, i tilfælde, hvor anvendelse heraf (sammenhængsmekanismen) er obligatorisk. Om afgrænsningen af sammenhængsmekanismen fremgår det endvidere, at i andre tilfælde af grænseoverskridende relevans bør mekanismen for samarbejde mellem den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder (artikel 60) finde anvendelse, og gensidig bistand (artikel 61) og fælles aktiviteter (artikel 62) kan gennemføres mellem de berørte tilsynsmyndigheder på bilateralt eller multilateralt grundlag, uden at det udløser sammenhængsmekanismen.

Med forordningens artikel 63 gøres det således – i modsætning til i dag – obligatorisk for tilsynsmyndighederne, og hvor det er relevant Kommissionen, at samarbejde om en række

sager, der i væsentlig grad påvirker et betydeligt antal registrerede i flere medlemsstater. I forhold til de situationer, hvor der i en medlemsstat måtte være mere end en tilsynsmyndighed, jf. artikel 51, stk. 3, henvises der til afsnit 7.1. om tilsynsmyndighed.

8.3.3.2. Udtalelse fra Databeskyttelsesrådet (artikel 64)

8.3.3.2.1. Databeskyttelsesforordningens artikel 64, stk. 1.

Det fremgår af forordningens artikel 64, stk. 1, at Databeskyttelsesrådet afgiver en udtalelse, når en kompetent tilsynsmyndighed har til hensigt at vedtage en af nedenstående foranstaltninger. Med henblik herpå sender den kompetente tilsynsmyndighed et udkast til afgørelse til rådet, når den:

> a) har til hensigt at vedtage en liste over typer af behandlingsaktiviteter, som er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse i henhold til artikel 35, stk. 4
>
> b) behandler et spørgsmål i henhold til artikel 40, stk. 7, om, hvorvidt et udkast til adfærdskodeks eller en ændring eller udvidelse af en adfærdskodeks overholder denne forordning
>
> c) har til hensigt at godkende kriterierne for akkreditering af et organ i henhold til artikel 41, stk. 3, eller et certificeringsorgan i henhold til artikel 43, stk. 3
>
> d) har til hensigt at vedtage standardbestemmelser om databeskyttelse som omhandlet i artikel 46, stk. 2, litra d), og i artikel 28, stk. 8
>
> e) har til hensigt at godkende kontraktbestemmelser som omhandlet i artikel 46, stk. 3, litra a), eller
>
> f) har til hensigt at godkende bindende virksomhedsregler som omhandlet i artikel 47.

Databeskyttelsesforordningens artikel 64, stk. 1, oplister således en række sagstyper, hvor en kompetent tilsynsmyndighed altid *skal* sende Databeskyttelsesrådet et udkast til udtalelse, inden myndigheden træffer afgørelse i sagen. Disse sagstyper er dermed på forhånd skønnede i væsentlig grad at kunne påvirke et betydeligt antal registrerede i flere medlemsstater.

Konsekvensen af manglende forelæggelse for Databeskyttelsesrådet i disse tilfælde, hvor anvendelsen af sammenhængsmekanismen er gjort obligatorisk, er endvidere, at de af til-

synsmyndigheden trufne foranstaltninger ikke er lovlige (gyldige), jf. præambelbetragtning nr. 138. Endvidere finder forordningens artikel 65 om tvistbilæggelse ved Databeskyttelsesrådet anvendelse, når en tilsynsmyndighed ikke efterlever artikel 64, stk. 1, jf. artikel 65, stk. 1, litra c, og afsnit 3.3. nedenfor.

8.3.3.2.2. Databeskyttelsesforordningens artikel 64, stk. 2.

Af forordningens artikel 64, stk. 2, fremgår det, at en tilsynsmyndighed, formanden for Databeskyttelsesrådet eller Kommissionen kan kræve, at ethvert almengyldigt spørgsmål eller ethvert spørgsmål, der har virkninger i mere end én medlemsstat, drøftes af Databeskyttelsesrådet med henblik på en udtalelse, navnlig hvis en kompetent tilsynsmyndighed ikke opfylder forpligtelserne vedrørende gensidig bistand, jf. artikel 61, eller vedrørende fælles aktiviteter, jf. artikel 62.

Endvidere fremgår det af præambelbetragtning nr. 136, 1. punktum, at Databeskyttelsesrådet – i forbindelse med anvendelsen af sammenhængsmekanismen – inden for en bestemt frist bør afgive en udtalelse, hvis det besluttes af et flertal af dets medlemmer, eller hvis en berørt tilsynsmyndighed eller Kommissionen anmoder herom.

Artikel 64, stk. 2, i forordningen kan synes at have karakter af en slags opsamlingsbestemmelse i forhold til bestemmelsens stk. 1, idet alle øvrige spørgsmål, der har virkninger i mere end én medlemsstat, kan kræves forelagt Databeskyttelsesrådet til udtalelse af en tilsynsmyndighed, formanden for Databeskyttelsesrådet eller Kommissionen.

Det er f.eks. i medfør af denne bestemmelse, at en medlemsstats tilsynsmyndighed, formanden for Databeskyttelsesrådet eller Kommissionen kan indbringe spørgsmål om en anden tilsynsmyndighed for rådet, hvis den er af den opfattelse, at denne anden tilsynsmyndighed ikke lever op til sine forpligtelser efter forordningen, jf. i den forbindelse således også henvisningen i bestemmelsen til artikel 61 om gensidig bistand og artikel 62 om fælles aktiviteter. Et eksempel herpå kunne være, at en tilsynsmyndighed afviser at imødekomme en anmodning om gensidig bistand fra en anden tilsynsmyndighed, selvom betingelserne for en afvisning i artikel 61, stk. 4, ikke er opfyldt.

Et andet eksempel på bestemmelsens anvendelse kan være, at en medlemsstats tilsynsmyndighed, formanden for Databeskyttelsesrådet eller Kommissionen er interesseret i at høre nærmere om en sag, som er under behandling hos en anden medlemsstats tilsynsmyndighed, fordi de finder, at sagen har virkninger i mere end én medlemsstat, men hvor denne anden tilsynsmyndighed ikke har vurderet, at dette er tilfældet.

Det er i øvrigt ikke en forudsætning for at kunne kræve noget forelagt, at der er tale om en sag, hvor der skal træffes afgørelse. Efter bestemmelsens ordlyd skal der blot være tale om ethvert alment spørgsmål eller et spørgsmål, der har virkning i mere end én medlemsstat som f.eks. en ny teknologi, der er under udvikling, eller et udkast til en EU-retsakt eller en tilstrækkelighedsafgørelse[806] fra Kommissionens side, som ønskes behandlet i Databeskyttelsesrådet.

8.3.3.2.3. Databeskyttelsesforordningens artikel 64, stk. 3.

Det fremgår af forordningens artikel 64, stk. 3, at Databeskyttelsesrådet, i de tilfælde, der er omhandlet i stk. 1 og 2, afgiver udtalelse om det spørgsmål, som det har fået forelagt, forudsat at det ikke allerede har afgivet en udtalelse om samme spørgsmål.

Endvidere fremgår det om udtalelsen fra Databeskyttelsesrådet, at denne vedtages inden for otte uger med simpelt flertal blandt medlemmerne af rådet, ligesom det fremgår, at fristen kan forlænges med yderligere seks uger under hensyntagen til spørgsmålets kompleksitet.

Herudover fremgår det, at et medlem af Databeskyttelsesrådet, som ikke har gjort indsigelse inden for en rimelig frist, der angives af formanden, anses for at være enig i det udkast til afgørelse, der i henhold til stk. 5 udsendes til medlemmerne af rådet.

Forordningens artikel 64, stk. 3, fastsætter således frister for, hvor lang tid Databeskyttelsesrådet må være om at komme med en udtalelse i de situationer, hvor rådet er forpligtet dertil efter artikel 64, stk. 1 og 2, ligesom bestemmelsen fastsætter, at medlemmerne af rådet skal gøre eventuelle indsigelser gældende inden for de fastsatte frister.

En frist på som udgangspunkt otte uger til vedtagelse af en udtalelse i Databeskyttelsesrådet synes at være en relativ kort frist henset til kompleksiteten af de spørgsmål, der kan blive forelagt rådet til udtalelse, jf. artikel 64, stk. 1 og 2. Hertil kommer, at der også vil skulle ske oversættelse af relevante oplysninger inden for otte ugers fristen, jf. artikel 64, stk. 5, som gennemgås nedenfor.

Som følge af otte ugers fristen må det antages, at Databeskyttelsesrådets behandling af sager efter artikel 64 vil være ret intensiv. De enkelte tilsynsmyndigheder vil derfor også være nødt til at give sagerne særlig prioritet, hvis de ønsker at gøre deres stemme gældende i rådet.

[806] En afgørelse fra Kommissionen i medfør af databeskyttelsesforordningens artikel 45, stk. 3.

8.3.3.2.4. Databeskyttelsesforordningens artikel 64, stk. 4.
Af forordningens artikel 64, stk. 4, fremgår det, at tilsynsmyndigheder og Kommissionen uden unødig forsinkelse elektronisk og i et standardformat sender Databeskyttelsesrådet alle relevante oplysninger, herunder et resumé af de faktiske omstændigheder, den foreslåede afgørelse, begrundelsen for vedtagelse af en sådan foranstaltning og andre berørte tilsynsmyndigheders synspunkter. Der henvises i den forbindelse også til artikel 67, som gennemgås nedenfor.

8.3.3.2.5. Databeskyttelsesforordningens artikel 64, stk. 5.
Det fremgår af forordningens artikel 64, stk. 5, at formanden for Databeskyttelsesrådet – uden unødig forsinkelse – *elektronisk* underretter:

a) medlemmerne af Databeskyttelsesrådet og Kommissionen om alle relevante oplysninger, som vedkommende har modtaget, i et standardformat. Sekretariatet for Databeskyttelsesrådet sørger efter behov for oversættelse af de relevante oplysninger, og
b) den tilsynsmyndighed, der er omhandlet i stk. 1 og 2, og Kommissionen om den pågældende udtalelse og offentliggør den.

8.3.3.2.6. Databeskyttelsesforordningens artikel 64, stk. 6.
Af forordningens artikel 64, stk. 6, fremgår det, at den kompetente tilsynsmyndighed ikke vedtager sit udkast til afgørelse omhandlet i stk. 1 i den periode, der er omhandlet i stk. 3.

8.3.3.2.7. Databeskyttelsesforordningens artikel 64, stk. 7.
Det fremgår af forordningens artikel 64, stk. 7, at den tilsynsmyndighed, der er omhandlet i stk. 1, tager videst muligt hensyn til Databeskyttelsesrådets udtalelse og senest to uger efter modtagelsen af udtalelsen giver formanden for rådet 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.

Formålet med, at tilsynsmyndigheden skal forelægge et ændret udkast til afgørelse må være, at rådet skal kunne kontrollere, om der er ændret i overensstemmelse med rådets udtalelse. Er dette ikke tilfældet, har formanden for rådet mulighed for at aktivere artikel 65 om tvistbilæggelse, der er omtalt nedenfor.

Hvis der i en given sag måtte være større indholdsmæssige forskelle på tilsynsmyndighedens oprindelige udkast til afgørelse og Databeskyttelsesrådets udtalelse, kan en frist på to uger til at sende formanden for rådet et ændret udkast til afgørelse synes kort.

8.3.3.2.8. Databeskyttelsesforordningens artikel 64, stk. 8.
Af forordningens artikel 64, stk. 8, fremgår det, at hvis den berørte tilsynsmyndighed inden for den frist, der er omhandlet i stk. 7, underretter formanden for Databeskyttelsesrådet om, at den helt eller delvist ikke agter at følge udtalelsen fra rådet, og den giver en relevant begrundelse herfor, finder artikel 65, stk. 1, anvendelse.

Er en tilsynsmyndighed således ikke enig i en udtalelse fra Databeskyttelsesrådet, og myndigheden derfor ikke agter at følge denne, skal spørgsmålet afgøres endeligt efter reglerne i artikel 65 om tvistbilæggelse, jf. nærmere herom nedenfor.

Det må antages, at forordningens artikel 65 kan aktiveres i alle tilfælde, hvor en berørt tilsynsmyndighed ikke agter at følge en udtalelse fra Databeskyttelsesrådet. Dette må gælde uanset, om den berørte tilsynsmyndighed har givet en (relevant) begrundelse for, at myndigheden ikke agter at følge en udtalelse fra rådet, selvom dette – efter bestemmelsens ordlyd – kunne tolkes at være et krav. Det vil umiddelbart savne mening, hvis en tilsynsmyndighed har mulighed for at undgå en tvistbilæggelse efter artikel 65 ved f.eks. bevidst at undlade at give en (relevant) begrundelse. Herudover må det i øvrigt forventes, at tilsynsmyndighederne i praksis vil komme med en begrundelse, hvis de måtte vælge ikke at følge en udtalelse fra rådet.

8.3.3.3. Tvistbilæggelse ved Databeskyttelsesrådet (artikel 65)
8.3.3.3.1. Databeskyttelsesforordningens artikel 65, stk. 1.
Det fremgår af forordningens artikel 65, stk. 1, at Databeskyttelsesrådet med henblik på at sikre korrekt og konsekvent anvendelse af databeskyttelsesforordningen i hvert enkelt tilfælde vedtager en *bindende* afgørelse i følgende tilfælde:

> a) hvis en berørt tilsynsmyndighed i et tilfælde som omhandlet i artikel 60, stk. 4, er fremkommet med en relevant og begrundet indsigelse mod et udkast til afgørelse udarbejdet af den ledende myndighed, eller den ledende myndighed har afvist en sådan indsigelse som værende uden relevans eller ubegrundet. Den bindende afgørelse skal vedrøre alle spørgsmål, der er genstand for den relevante og begrundede indsigelse, navnlig hvorvidt denne forordning er overtrådt
>
> b) hvis der er uenighed om, hvilken af de berørte tilsynsmyndigheder der er kompetent med hensyn til hovedvirksomheden
>
> c) hvis en kompetent tilsynsmyndighed ikke anmoder om udtalelse fra Databeskyttelsesrådet i de tilfælde, der er omhandlet i artikel 64, stk. 1,

eller ikke følger Databeskyttelsesrådets udtalelse udstedt i henhold til artikel 64. I så fald kan enhver berørt tilsynsmyndighed eller Kommissionen indbringe spørgsmålet for Databeskyttelsesrådet.

Herudover fremgår det af præambelbetragtning nr. 136, 2. punktum, at Databeskyttelsesrådet bør tillægges beføjelse til at vedtage juridisk bindende afgørelser i tilfælde af tvister mellem tilsynsmyndigheder. Det fremgår endvidere af præambelbetragtning nr. 136, sidste punktum, at rådet til ovennævnte formål, i princippet med et flertal på to tredjedele af sine medlemmer, bør vedtage juridisk bindende afgørelser i klart angivne tilfælde, hvor der er modstridende synspunkter blandt tilsynsmyndighederne, særlig i samarbejdsmekanismen mellem den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder om en sags realitet, navnlig om hvorvidt der foreligger en overtrædelse af denne forordning.

Af forordningens artikel 65, stk. 1, fremgår det således, at Databeskyttelsesrådet i en række tilfælde kan træffe afgørelser, der er bindende for de berørte tilsynsmyndigheder. Dette er bl.a. tilfældet, hvis tilsynsmyndigheder, der samarbejder efter artikel 60 ikke kan blive enige om et udkast til en afgørelse, eller hvis en tilsynsmyndighed ikke følger en udtalelse fra rådet i henhold til artikel 64.

Det, at tilsynsmyndighederne – i sager der påvirker registrerede i flere medlemsstater – fremover kan blive underlagt afgørelser fra et flertal (jf. gennemgangen af stk. 2 og 3 nedenfor) af de øvrige tilsynsmyndigheder (medlemmer af Databeskyttelsesrådet) i EU, er meget anderledes, end den retstilstand, der har været gældende med databeskyttelsesdirektivet. En konsekvens af reglen kan således f.eks. blive, at en dansk virksomhed, der opererer i flere medlemsstater, fremadrettet kan blive underlagt en afgørelse, som Datatilsynet ikke er enig i, men som tilsynet alligevel bliver nødt til at håndhæve over for virksomheden.

Ovennævnte betyder også, at der vil kunne forekomme situationer, hvor det kan vise sig vanskeligt for Datatilsynet at rådgive en dansk virksomhed om en problemstilling, der har et grænse-overskridende element. En sådan rådgivning vil således forudsætte, at Datatilsynet har et vist kendskab til, hvordan man ser på problemstillingen i de øvrige medlemsstater.

8.3.3.3.2. Databeskyttelsesforordningens artikel 65, stk. 2.

Af forordningens artikel 65, stk. 2, fremgår det, at den afgørelse, der er omhandlet i stk. 1, vedtages inden for en måned fra forelæggelsen af spørgsmålet med et flertal på to tredjedele blandt medlemmerne af Databeskyttelsesrådet. Det fremgår endvidere, at fristen kan forlænges med yderligere en måned på grund af spørgsmålets kompleksitet. Endelig frem-

går det af bestemmelsen, at afgørelsen i stk. 1 skal være begrundet og rettet til den ledende tilsynsmyndighed og alle de berørte tilsynsmyndigheder og have bindende virkning for dem.

En frist på som udgangspunkt en måned til at træffe afgørelse i en sag, der berører registrerede i flere medlemsstater, kan synes meget kort. Rådets behandling af en sag efter artikel 65, stk. 2, må derfor antages at ville blive endnu mere intensiv, end rådets forberedelse af udtalelser efter artikel 64. Tilsynsmyndighederne vil dermed også her være nødt til at give sagerne særlig prioritet.

8.3.3.3.3. Databeskyttelsesforordningens artikel 65, stk. 3.
Det fremgår af forordningens artikel 65, stk. 3, at hvis Databeskyttelsesrådet ikke har været i stand til at træffe en afgørelse inden for de i stk. 2 omhandlede frister, vedtager rådet sin afgørelse senest to uger efter udløbet af den anden måned som omhandlet i stk. 2 med simpelt flertal blandt Databeskyttelsesrådets medlemmer. Om tilfælde af stemmelighed blandt medlemmerne af rådet fremgår det tillige, at formandens stemme i disse situationer er udslagsgivende.

Artikel 65, stk. 3, er tiltænkt de situationer, hvor det ikke har været muligt, inden for fristerne i stk. 2, at opnå to tredjedeles flertal for en afgørelse i rådet. I disse situationer vil Databeskyttelsesrådet i stedet kunne træffe afgørelse med simpelt flertal. Hvis der er stemmelighed, vil det være formanden for rådets stemme, der vil være udslagsgivende.

I yderste konsekvens kan artikel 65, stk. 3, når formandens stemme er udslagsgivende, i tilfælde af stemmelighed, føre til, at halvdelen af medlemmerne af Databeskyttelsesrådet kan tvinge den anden halvdel af medlemmerne til at følge en afgørelse, som de ikke er enige i.

8.3.3.3.4. Databeskyttelsesforordningens artikel 65, stk. 4.
Af forordningens artikel 65, stk. 4, fremgår det, at de berørte tilsynsmyndigheder ikke må vedtage en afgørelse om et spørgsmål, der er forelagt for Databeskyttelsesrådet i henhold til stk. 1, i løbet af de i stk. 2 og 3 omhandlede perioder.

8.3.3.3.5. Databeskyttelsesforordningens artikel 65, stk. 5.
Det fremgår af forordningens artikel 65, stk. 5, at formanden for Databeskyttelsesrådet uden unødig forsinkelse meddeler den i stk. 1 omhandlede afgørelse til de berørte tilsynsmyndigheder, og at formanden ligeledes underretter Kommissionen herom.

Endvidere fremgår det, at afgørelsen straks offentliggøres på Databeskyttelsesrådets hjemmeside, når tilsynsmyndigheden har meddelt den endelige afgørelse, jf. stk. 6, der er nærmere omtalt umiddelbart nedenfor.

Det må antages, at en offentliggørelse på Databeskyttelsesrådets hjemmeside skal ske i overensstemmelse med de regler, som EDPS[807] er underlagt. Dette skyldes, at EDPS skal fungere som sekretariat for Databeskyttelsesrådet. Muligheden for offentliggørelse af f.eks. fortrolige personoplysninger må således også skulle afgøres efter disse regler.

8.3.3.3.6. Databeskyttelsesforordningens artikel 65, stk. 6.

Af forordningens artikel 65, stk. 6, fremgår det, at den ledende tilsynsmyndighed eller efter omstændighederne den tilsynsmyndighed, til hvem en klage er indgivet, vedtager sin endelige afgørelse på grundlag af den i artikel 65, stk. 1, omhandlede afgørelse uden unødig forsinkelse og senest en måned efter, at Databeskyttelsesrådet har meddelt sin afgørelse.

Herudover fremgår det, at den ledende tilsynsmyndighed eller efter omstændighederne den tilsynsmyndighed, til hvem klagen er indgivet, underretter Databeskyttelsesrådet om datoen for meddelelse af sin endelige afgørelse til henholdsvis den dataansvarlige eller databehandleren og den registrerede.

Det fremgår endvidere, at den berørte tilsynsmyndigheds endelige afgørelse vedtages i henhold til artikel 60, stk. 7, 8 og 9.

Af bestemmelsen fremgår tillige, at den endelige afgørelse skal indeholde en henvisning til den afgørelse, der er omhandlet i artikel 65, stk. 1, og angive, at den i nævnte stykke omhandlede afgørelse vil blive offentliggjort på Databeskyttelsesrådets hjemmeside i overensstemmelse med artikel 65, stk. 5.

Endelig fremgår det, at den i artikel 65, stk. 1, omhandlede afgørelse skal vedlægges den endelige afgørelse.

8.3.3.4. Hasteprocedure (artikel 66)

8.3.3.4.1. Databeskyttelsesforordningens artikel 66, stk. 1.

Det fremgår af forordningens artikel 66, stk. 1, at når en berørt tilsynsmyndighed under ekstraordinære omstændigheder mener, at det er nødvendigt at handle omgående for at beskytte registreredes rettigheder og frihedsrettigheder, kan myndigheden uanset den i artikel 63, 64 og 65 omhandlede sammenhængsmekanisme eller den i artikel 60 omhandlede

[807] Den Europæiske Tilsynsførende for Databeskyttelse.

procedure omgående træffe foreløbige foranstaltninger, der skal have retsvirkning på dens eget område med en angivet gyldighedsperiode, som ikke må overstige tre måneder.

Om tilfælde, hvor en berørt tilsynsmyndighed benytter sig af ovennævnte procedure, fremgår det endvidere, at tilsynsmyndigheden i sådanne tilfælde straks skal meddeler de andre berørte tilsynsmyndigheder, Databeskyttelsesrådet og Kommissionen om disse foranstaltninger og en begrundelse for vedtagelsen heraf.

Af præambelbetragtning nr. 137 fremgår det, at det kan være nødvendigt at handle omgående for at beskytte registreredes rettigheder og frihedsrettigheder, navnlig hvis der er fare for væsentlig vanskeliggørelse af håndhævelsen af en registrerets rettigheder. På baggrund heraf fremgår det tillige, at en tilsynsmyndighed derfor bør kunne vedtage behørigt begrundede foreløbige foranstaltninger på sit område med en angivet gyldighedsperiode, der ikke bør overstige tre måneder.

Ved en gennemgang af de situationer, der kan medføre et krav om en udtalelse efter forordningens artikel 64, er det umiddelbart svært at give et eksempel på, hvornår det måtte være nødvendigt at handle omgående for at beskytte de registreredes rettigheder og frihedsrettigheder, jf. artikel 66, stk. 1.

Det er nok mere sandsynligt, at der i en sag, der behandles efter artikel 60, kan opstå en situation, hvor det er nødvendigt at handle omgående for at beskytte de registreredes rettigheder og frihedsrettigheder, jf. artikel 66, stk. 1. Et eksempel herpå kunne måske være, at en ledende tilsynsmyndighed finder det nødvendigt omgående at forbyde en virksomhed, der opererer i flere medlemsstater, at foretage en given behandling af personoplysninger, da en fortsat behandling vil kunne føre til, at oplysninger om de registrerede potentielt ulovligt vil blive videregivet til en anden virksomhed eller lignende.

8.3.3.4.2. Databeskyttelsesforordningens artikel 66, stk. 2.

Af forordningens artikel 66, stk. 2, fremgår det, at hvis en tilsynsmyndighed har vedtaget en foranstaltning i henhold til stk. 1 og mener, at der omgående skal vedtages endelige foranstaltninger, kan den anmode om en hasteudtalelse eller en hurtig bindende afgørelse fra Databeskyttelsesrådet, idet tilsynsmyndigheden begrunder anmodningen om en sådan udtalelse eller afgørelse.

Artikel 66, stk. 2, giver således mulighed for, at den tilsynsmyndighed, der har vedtaget en midlertidig foranstaltning efter stk. 1, også kan anmode om en hasteudtalelse eller en hurtigt bindende afgørelse.

8.3.3.4.3. Databeskyttelsesforordningens artikel 66, stk. 3.
Det fremgår af forordningens artikel 66, stk. 3, at enhver tilsynsmyndighed kan anmode om en hasteudtalelse eller efter omstændighederne en hurtig bindende afgørelse, fra Databeskyttelsesrådet, hvis en kompetent tilsynsmyndighed ikke har truffet de fornødne foranstaltninger i en situation, hvor det er nødvendigt at handle omgående for at beskytte registreredes rettigheder og frihedsrettigheder, idet tilsynsmyndigheden begrunder anmodningen om en sådan udtalelse eller afgørelse, herunder behovet for at handle omgående.

Med artikel 66, stk. 3, gives der – som en slags pendant til stk. 2 – mulighed for, at også andre tilsynsmyndigheder kan anmode om en hasteudtalelse eller en hurtigt bindende afgørelse, hvis den kompetente tilsynsmyndighed ikke af sig selv træffer de fornødne foranstaltninger efter stk. 1.

8.3.3.4.4. Databeskyttelsesforordningens artikel 66, stk. 4.
Af forordningens artikel 66, stk. 4, fremgår det, at uanset artikel 64, stk. 3, og artikel 65, stk. 2, vedtages en hasteudtalelse eller en hurtig bindende afgørelse som omhandlet i artikel 66, stk. 2 og 3, inden for to uger med simpelt flertal blandt medlemmerne af Databeskyttelsesrådet.

Udgangspunktet under hasteproceduren er således, at udtalelser og bindende afgørelser vedtages med simpelt flertal i alle tilfælde. I modsætning til artikel 65, stk. 3, situationerne fremgår det ikke af artikel 66, stk. 4, hvad der skal ske i tilfælde af stemmelighed.

8.3.3.5. Udveksling af oplysninger (artikel 67)
Det følger af forordningens artikel 67, at Kommissionen kan vedtage gennemførelsesretsakter af generel karakter med henblik på nærmere at angive ordningerne for elektronisk udveksling af oplysninger mellem tilsynsmyndigheder og mellem tilsynsmyndigheder og Databeskyttelsesrådet, navnlig det standardformat, der er omhandlet i artikel 64.

Endvidere fremgår det, at disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 92, stk. 2.

I præambelbetragtning nr. 168 gentages det herudover bl.a., at undersøgelsesproceduren skal anvendes til vedtagelse af gennemførelsesretsakter om ordninger for elektronisk udveksling af oplysninger mellem tilsynsmyndigheder og mellem tilsynsmyndigheder og Databeskyttelsesrådet.

Det må forventes, at Kommissionen vil benytte sig af sine beføjelser til at vedtage gennemførelsesretsakter med henblik på nærmere at angive ordningerne for elektronisk udveksling af oplysninger.

8.3.4. Overvejelser

Som nævnt ovenfor findes der hverken i databeskyttelsesdirektivet eller persondataloven bestemmelser, som svarer til databeskyttelsesforordningens artikel 63-67 om sammenhæng.

Selvom tilsynsmyndighederne allerede nu i et vist omfang – på frivillig basis – har samarbejdet om en ensartet anvendelse af databeskyttelsesdirektivet i enkeltsager, må forordningens regler om en sammenhængsmekanisme forventes at skabe en ny virkelighed for især tilsynsmyndighederne.

Dette skyldes bl.a., at der – jf. gennemgangen ovenfor – med databeskyttelsesforordningens artikel 64-66 fastsættes detaljerede regler for, hvilke typer af tilsynsafgørelser, der skal og kan forelægges for Databeskyttelsesrådet til udtalelse, inden de bliver iværksat, ligesom der fastsættes regler for, i hvilke situationer Databeskyttelsesrådet kan træffe afgørelser med bindende virkning for tilsynsmyndighederne og dermed også de berørte virksomheder m.fl. Der kan således med forordningens regler opstå situationer, hvor en dansk virksomhed, der opererer i flere medlemsstater, kan blive underlagt en afgørelse, som det danske datatilsyn ikke er enig i, men som tilsynet alligevel bliver nødt til at håndhæve over for virksomheden.

Tilsynsmyndighederne må på denne baggrund indstille sig på at skulle samarbejde om en ensartet anvendelse af forordningen, i markant flere sager, end det hidtil er sket på frivillig basis efter databeskyttelsesdirektivet.

Som følge af Databeskyttelsesrådets øgede beføjelser – set i forhold til Artikel 29-gruppens nuværende beføjelser – vil det være særdeles vigtigt, at Datatilsynet i endnu videre omfang end i dag bliver en aktiv spiller i rådet, og dermed giver sagerne prioritet, herunder bl.a. henset til de relativt korte tidsfrister i artikel 64-66.[808]

Det fremgår i den forbindelse i øvrigt også af databeskyttelsesforordningens artikel 57, stk. 1, litra t, at tilsynsmyndigheden skal bidrage til Databeskyttelsesrådets aktiviteter. Hvis en tilsynsmyndighed forsømmer sig herimod efter enten de andre tilsynsmyndigheders, formanden for Databeskyttelsesrådet eller Kommissionens opfattelse, vil de kunne indbringe

[808] Se også Peter Blume, Den nye persondataret (2016), s. 156.

dette spørgsmål og tilsynsmyndigheden for Databeskyttelsesrådet, og i yderste konsekvens vil også Kommissionen kunne anlægge en traktatkrænkelsessag mod den medlemsstat, hvis tilsynsmyndighed ikke lever op til sit ansvar.

8.4. Databeskyttelsesrådet, artikel 68 og artikel 70-76

8.4.1. Præsentation

Databeskyttelsesforordningens kapitel VII indeholder på den baggrund regler om samarbejde mellem tilsynsmyndighederne i EU. Reglerne foreskriver forskellige former for samarbejde, herunder regler om fælles beslutningstagen i visse sager, gensidig bistand og fælles aktiviteter, ligesom kapitlet indeholder regler om en såkaldt "sammenhængsmekanisme", som skal sikre en ensartet anvendelse af forordningen, og som betyder af Det Europæiske Databeskyttelsesråd (herefter Databeskyttelsesrådet) i visse tilfælde skal udstede vejledende udtalelser og i visse tilfælde træffe afgørelser, som er bindende for tilsynsmyndighederne. Databeskyttelsesrådet, som sammensættes af medlemsstaternes tilsynsmyndigheder, skal erstatte den eksisterende Artikel 29-gruppe, som er oprettet i henhold til det gældende databeskyttelsesdirektiv.

I det følgende foretages en gennemgang af reglerne i afdeling 3 i forordningens kapitel VII om Databeskyttelsesrådet. Forordningens artikel 68 og artikel 70-76 regulerer rådets opgaver, rapporter, procedure, fortrolighed, formanden, formandens opgaver, rådets sekretariat og fortrolighed.

8.4.2. Gældende ret

8.4.2.1. Artikel 29-gruppen

Efter artikel 29, stk. 1, i databeskyttelsesdirektivet nedsættes der en "gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger", den såkaldte Artikel 29-gruppe. Gruppen er rådgivende og uafhængig.

Af direktivets artikel 29, stk. 2, fremgår det, at gruppen 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.

Hvert medlem af gruppen udpeges af den institution eller den eller de myndigheder, det repræsenterer. Når en medlemsstat har udpeget flere tilsynsmyndigheder, udnævner disse en fælles repræsentant. Det samme gælder de myndigheder, der er oprettet for fællesskabs-

institutionerne og -organerne. For Danmarks vedkommende varetages medlemskabet af Datatilsynets direktør.

Det er endvidere i direktivets artikel 29, stk. 3, fastsat, at gruppen træffer sine afgørelser med simpelt flertal blandt repræsentanterne for tilsynsmyndighederne. Gruppen vælger selv sin formand, hvis mandat gælder for en periode af to år og kan fornyes, jf. direktivets artikel 29, stk. 4. Det kan i den forbindelse nævnes, at gruppen siden sin oprettelse ikke har haft en formand fra de nordiske lande.[809]

Gruppens sekretariatsopgaver varetages ifølge direktivets artikel 29, stk. 5, af Kommissionen, og gruppen fastsætter selv sin forretningsorden, jf. direktivets artikel 29, stk. 6.

I Artikel 29-gruppens nuværende forretningsorden, der er vedtaget den 15. februar 2010, er der fastsat regler om gruppens nedsættelse og opgaver (artikel 1), medlemmer (artikel 2), valg af formand og næstformand (artikel 3), sekretariatets opgaver (artikel 4), mødefrekvens og -sted (artikel 5-6), dagsorden (artikel 7), deltagelse i møderne (artikel 8-9), quorum (artikel 10), organisering af drøftelserne (artikel 11), beslutninger (artikel 12), skriftlig procedure (artikel 13), begrundelser (artikel 14), årsrapport (artikel 15), nedsættelse af undergrupper og udpegning af de såkaldte "rapporteurs" (artikel 16), stemmeafgivning (artikel 17), referat (artikel 18) samt om ændring af forretningsordenen (artikel 19).

Efter direktivets artikel 29, stk. 7, behandler gruppen de spørgsmål, der sættes på dagsordenen af dens formand, enten på formandens initiativ, efter anmodning fra en repræsentant for tilsynsmyndighederne eller efter anmodning fra Kommissionen.

Gruppen har i medfør af direktivets artikel 30, stk. 1, følgende opgaver:

a) at undersøge ethvert spørgsmål vedrørende anvendelse af de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, med henblik på at bidrage til en ensartet anvendelse heraf

b) at give Kommissionen en udtalelse om beskyttelsesniveauet i Fællesskabet og i tredjelande

c) at rådgive Kommissionen om ethvert udkast til ændring af dette direktiv og om, hvilke supplerende eller specifikke foranstaltninger der bør træffes for at sikre fysiske personers rettigheder og frihedsrettigheder

[809] Peter Blume, Den nye persondataret (2016), s 158.

for så vidt angår behandling af personoplysninger, samt om ethvert andet udkast til fællesskabsforanstaltninger, der har indvirkning på sådanne rettigheder og frihedsrettigheder

d) at afgive udtalelse om de adfærdskodekser, der udarbejdes på fællesskabsplan.

Det følger af direktivets artikel 30, stk. 2, at hvis gruppen konstaterer forskelle mellem medlemsstaternes lovgivning eller praksis, der kan være til fare for en ensartet beskyttelse af personer i forbindelse med behandling af personoplysninger inden for Fællesskabet, underretter den Kommissionen herom.

Direktivets artikel 30, stk. 3, fastslår, at gruppen på eget initiativ kan fremsætte henstillinger om ethvert spørgsmål vedrørende beskyttelsen af personer i forbindelse med behandling af personoplysninger inden for Fællesskabet.

Gruppens udtalelser og henstillinger forelægges i medfør af direktivets artikel 30, stk. 4, for Kommissionen og for det udvalg, der er nedsat i medfør af artikel 31.[810]

Efter direktivets artikel 30, stk. 5, underretter Kommissionen gruppen om, hvorledes den har taget hensyn til dens udtalelser og henstillinger. Kommissionen udarbejder med henblik herpå en beretning, som også forelægges for Europa-Parlamentet og Rådet. Denne beretning offentliggøres.

Endelig er det fastsat i direktivets artikel 30, stk. 6, at gruppen udarbejder en årsberetning om situationen vedrørende beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger inden for Fællesskabet og i tredjelande. Gruppen forelægger beretningen for Europa-Parlamentet, Rådet og Kommissionen. Beretningen offentliggøres.

Artikel 29-gruppen har i tidens løb udgivet en lang række henstillinger, udtalelser mv., der, selv om de ikke er bindende for medlemsstaterne, formentlig har haft en vis normerende effekt for de nationale tilsynsmyndigheder og må dermed antages at have medvirket til at øge graden af harmonisering af udmøntningen af direktivets regler i medlemsstaterne.

[810] Der er i direktivets artikel 31, stk. 1, fastsat, at Kommissionen bistås af et udvalg, der består af repræsentanter for medlemsstaternes regeringer, og som har Kommissionens repræsentant som formand. For Danmarks vedkommende varetages medlemskabet af Justitsministeriet.

Der ses i øvrigt flere eksempler på, at medlemsstaterne på frivillig basis i regi af Artikel 29-gruppen (eller undergrupper dertil) har samarbejdet om problemstillinger, der har haft grænseoverskridende elementer.

8.4.3. Databeskyttelsesforordningen

8.4.3.1. Det Europæiske Databeskyttelsesråd (artikel 68)

8.4.3.1.1. Databeskyttelsesforordningens artikel 68, stk. 1

Forordningens artikel 68, stk. 1, opretter Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") som et EU-organ med status som juridisk person.

Af præambelbetragtning nr. 139 fremgår bl.a., at Databeskyttelsesrådet – med henblik på at fremme, at forordningen anvendes på en ensartet måde – bør oprettes som et uafhængigt EU-organ. Databeskyttelsesrådet bør for at kunne opfylde sine målsætninger have status som juridisk person. Det fremgår endvidere, at Databeskyttelsesrådet bør erstatte Artikel 29-gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved databeskyttelsesdirektivet.

Det bemærkes, at det forhold, at Databeskyttelsesrådet får status som juridisk person, indebærer, at rådet får evnen til at forpligte sig, dels ved indgåelse af aftaler med tredjelande eller internationale organisationer dels ved indgåelse af almindelige kontrakter (køb, leje mv.).

8.4.3.1.2. Databeskyttelsesforordningens artikel 68, stk. 2-5

Rådet repræsenteres efter forordningens artikel 68, stk. 2, af sin formand og sammensættes af chefen for en tilsynsmyndighed i hver medlemsstat og af Den Europæiske Tilsynsførende for Databeskyttelse (EDPS)[811] eller deres respektive repræsentanter, jf. artikel 68, stk. 3.

Det følger af forordningens artikel 68, stk. 4, at hvis mere end én tilsynsmyndighed i en medlemsstat er ansvarlig for at føre tilsyn med af anvendelsen af bestemmelserne i forordningen, udnævnes en fælles repræsentant i henhold til den pågældende medlemsstats nationale ret.

Efter forordningens artikel 68, stk. 5, har Kommissionen ret til at deltage i Databeskyttelsesrådets aktiviteter og møder. Det er dog præciseret, at Kommissionen deltager uden stemmeret, som det også er tilfældet efter direktivet.

[811] Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) fører tilsyn med den behandling af personoplysninger, der foretages af EU's institutioner og organer.

Det følger endvidere af stk. 5, at Kommissionen udpeger en repræsentant, og at formanden for Databeskyttelsesrådet underretter Kommissionen om aktiviteterne i Databeskyttelsesrådet.

Reglerne i forordningens artikel 68, stk. 2-5, svarer i meget vidt omfang til bestemmelser i direktivets artikel 29.

8.4.3.1.3. Databeskyttelsesforordningens artikel 68, stk. 6

Det følger af forordningens artikel 68, stk. 6, at EDPS i de i artikel 65 omhandlede tilfælde (tvistbilæggelse ved Databeskyttelsesrådet) kun har stemmeret i forbindelse med afgørelser, der vedrører principper og bestemmelser, som gælder for Unionens institutioner, organer, kontorer og agenturer, og som indholdsmæssigt er i overensstemmelse med forordningens principper og bestemmelser.

Dette sikrer, at EDPS i afgørelsessager efter artikel 65 alene har stemmeret i de tilfælde, hvor afgørelsen har direkte betydning for EDPS' virkeområde.

8.4.3.2. Opgaver (artikel 70, stk. 1, litra a-y)

8.4.3.2.1. Databeskyttelsesforordningens artikel 70, stk. 1,litra a og litra t

Af forordningens artikel 70, stk. 1, litra a, fremgår det, at Databeskyttelsesrådet på eget initiativ eller, når det er relevant, efter anmodning fra Kommissionen navnlig skal føre tilsyn med og sikre korrekt anvendelse af denne forordning i de tilfælde, der er omhandlet i forordningens artikel 64 (udtalelse om tilsynsmyndigheders påtænkte aktiviteter) og artikel 65 (om tvistbilæggelse), uden at dette berører de nationale tilsynsmyndigheders opgaver.

Endvidere fremgår det af forordningens artikel 70, stk. 1, litra t, at rådet skal afgive udtalelser om tilsynsmyndigheders udkast til afgørelse i overensstemmelse med den sammenhængsmekanisme, der er omhandlet i artikel 64, stk. 1, og om sager, der er forelagt i henhold til artikel 64, stk. 2, og udstede bindende afgørelser i henhold til artikel 65, herunder i de tilfælde, der er omhandlet i artikel 66

For en nærmere gennemgang af forordningens artikel 64 og artikel 65 henvises til den såkaldte "sammenhængsmekanisme" i forordningens kapitel VII, afdeling 2 (artikel 63-67).

8.4.3.2.2. Databeskyttelsesforordningens artikel 70, stk. 1, litra b-c

Databeskyttelsesrådet skal ifølge forordningens artikel 70, stk. 1, litra b, rådgive Kommissionen om ethvert spørgsmål vedrørende beskyttelse af personoplysninger i EU, herunder om ethvert forslag til ændring af forordningen.

Endvidere følger det af forordningens artikel 70, stk. 1, litra c, at rådet skal rådgive Kommissionen om format og procedurer for videregivelse af oplysninger mellem dataansvarlige, databehandlere og tilsynsmyndigheder vedrørende bindende virksomhedsregler.

8.4.3.2.3. Databeskyttelsesforordningens artikel 70, stk. 1,litra d

Det fremgår af forordningens artikel 70, stk. 1, litra d, at Databeskyttelsesrådet skal udstede retningslinjer, henstillinger og bedste praksis vedrørende procedurer for sletning af link til og kopier eller gengivelser af personoplysninger fra offentligt tilgængelige kommunikationstjenester som omhandlet i artikel 17, stk. 2.

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.

Der henvises i øvrigt til afsnit 4.7. for en nærmere gennemgang af artikel 17.

8.4.3.2.4. Databeskyttelsesforordningens artikel 70, stk. 1,litra e-m

Af forordningens artikel 70, stk. 1, litra e, fremgår det, 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. Disse områder er: kriterierne og betingelserne for afgørelser baseret på profilering i henhold til artikel 22, stk. 2 (litra f), 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 (litra g), 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 (litra h), kriterierne for og kravene til overførsel af personoplysninger baseret på bindende virksomhedsregler, som dataansvarlige overholder, og bindende virksomhedsregler, som databehandlere overholder, og vedrørende yderligere krav til at sikre beskyttelse af de berørte registreredes personoplysninger som omhandlet i artikel 47 (litra i), kriterierne for og kravene til overførsel af personoplysninger på grundlag af artikel 49, stk. 1 (litra j), tilsynsmyndighedernes anvendelse af foranstaltninger, jf. artikel 58, stk. 1, 2 og 3, og fastsættelse af administrative bøder i henhold til

artikel 83 (litra k) samt fastlæggelse af fælles procedurer for fysiske personers indberetning af overtrædelser af denne forordning, jf. artikel 54, stk. 2 (litra m).

De omhandlede retningslinjer mv. er ikke bindende for medlemsstaterne, men vil formentlig få en 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.

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.

8.4.3.2.5. Databeskyttelsesforordningens artikel 70, stk. 1, litra n-q og litra x
Databeskyttelsesrådet skal ifølge forordningens artikel 70, stk. 1, litra n, tilskynde til udarbejdelse af adfærdskodekser og fastlæggelse af certificeringsmekanismer for databeskyttelse og databeskyttelsesmærkninger og -mærker i henhold til artikel 40 og 42.

Endvidere skal rådet efter forordningens artikel 70, stk. 1, litra o, foretage akkreditering af certificeringsorganer og regelmæssig revision heraf i henhold til artikel 43 og føre et offentligt register over akkrediterede organer i henhold til artikel 43, stk. 6, og over de akkrediterede dataansvarlige eller databehandlere i tredjelande i henhold til artikel 42, stk. 7.

Databeskyttelsesrådet skal desuden angive de krav, der er omhandlet i artikel 43, stk. 3, med henblik på akkreditering af certificeringsorganer i henhold til artikel 42, jf. forordningens artikel 70, stk. 1, litra p.

Herudover følger det af forordningens artikel 70, stk. 1 litra q, at rådet skal afgive udtalelse til Kommissionen om de certificeringskrav, der er omhandlet i artikel 43, stk. 8.

Det fremgår endelig af forordningens artikel 70, stk. 1, litra x, at Databeskyttelsesrådet skal afgive udtalelser om adfærdskodekser, der udarbejdes på EU-plan, jf. artikel 40, stk. 9.

Der henvises til afsnit 5.22.-5.25. for en nærmere gennemgang af forordningens artikel 40-43 om adfærdskodekser og certificering.

8.4.3.2.6. Databeskyttelsesforordningens artikel 70, stk. 1,litra r-s
Af forordningens artikel 70, stk. 1, litra r, fremgår, at Databeskyttelsesrådet skal afgive udtalelse til Kommissionen om de ikoner, der er omhandlet i artikel 12, stk. 7.

Rådet skal endvidere efter forordningens artikel 70, stk. 1, litra s, afgive udtalelse til Kommissionen med henblik på vurdering af tilstrækkeligheden af beskyttelsesniveauet i et tredjeland eller en international organisation, herunder vurdering af, om et tredjeland, et område eller en eller flere specifikke sektorer i det pågældende tredjeland, eller en international organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau. Til dette formål forelægger Kommissionen Databeskyttelsesrådet al nødvendig dokumentation vedrørende tredjelandet, området eller den specifikke sektor, eller den internationale organisation, herunder korrespondance med regeringen i tredjelandet,

8.4.3.2.7. Databeskyttelsesforordningens artikel 70, stk. 1, litra u-w

Ifølge forordningens artikel 70, stk. 1, litra u, skal Databeskyttelsesrådet fremme samarbejdet og effektiv bilateral og multilateral udveksling af oplysninger og bedste praksis mellem tilsynsmyndighederne.

Endvidere skal rådet fremme fælles uddannelsesprogrammer og udveksling af personale mellem tilsynsmyndighederne og i relevante tilfælde med tilsynsmyndighederne i tredjelande eller med internationale organisationer, jf. forordningens artikel 70, stk. 1, litra v.

Rådet skal herudover ifølge forordningens artikel 70, stk. 1, litra w, fremme udveksling af viden og dokumentation vedrørende databeskyttelseslovgivning og -praksis med datatilsynsmyndigheder over hele verden.

8.4.3.2.8. Databeskyttelsesforordningens artikel 70, stk. 1, litra y

Databeskyttelsesrådet skal endelig ifølge forordningens artikel 70, stk. 1, litra y, føre et offentligt tilgængeligt elektronisk register over afgørelser truffet af tilsynsmyndigheder og domstole om spørgsmål, der er blevet behandlet i sammenhængsmekanismen.

8.4.3.2.9. Sammenfattende om Databeskyttelsesrådets opgaver

Reglerne om Databeskyttelsesrådets opgaver viderefører, uddyber og kodificerer i et vist omfang de opgaver, som Artikel 29-gruppen har efter direktivet. Opgaven med at rådgive og underrette Kommissionen samt at afgive henstillinger er således også et centralt element i Artikel 29-gruppens opgavekatalog efter artikel 30, jf. ovenfor.

En del af Databeskyttelsesrådets opgaver er imidlertid nye. Det gælder for eksempel forpligtelsen til at udstede retningslinjer, henstillinger og bedste praksis i forhold til reglerne om profilering (litra f), anmeldelse af brud på datasikkerheden (litra g og litra h), akkreditering af certificeringsorganer (litra o) og ikoner (litra r). Databeskyttelsesrådet skal også i højere grad følge og kontrollere de nationale tilsynsmyndigheders måde at håndhæve forordningens regler på. Som eksempler herpå kan nævnes forpligtelsen til at udstede ret-

ningslinjer vedrørende anvendelse af foranstaltninger, jf. artikel 58, stk. 1, 2. og 3, og fastsættelse af administrative bøder i henhold til artikel 83 (litra k), forpligtelsen til at gennemgå den praktiske anvendelse af de retningslinjer og henstillinger og den bedste praksis, der er omhandlet i litra e og f (litra l), samt pligten til at fremme samarbejdet og effektiv bilateral og multilateral udveksling af oplysninger og bedste praksis mellem tilsynsmyndighederne (litra u).

Der, hvor Databeskyttelsesrådets opgaver må siges at være væsensforskellige fra Artikel 29-gruppens, og hvormed der sker den mest markante styrkelse af rådet, er dog først og fremmest i relation til de udtalelser, som de nationale tilsynsmyndigheder skal indhente i henhold til artikel 64, samt i forhold til rådets nye afgørelseskompetence efter artikel 65 om tvistbilæggelse og rådets tilsynsforpligtelse i den forbindelse, jf. artikel 70, stk. 1, litra a og t.

Reguleringen af Databeskyttelsesrådets opgaver er samtidig langt mere detaljeret, end det er tilfældet for Artikel 29-gruppen, hvilket muligvis bl.a. har baggrund i de styrkede krav til ensartet og konsekvent anvendelse af forordningen, som rådet indtager en afgørende rolle i at sikre. Det skal i den forbindelse nævnes, at formuleringen af Databeskyttelsesrådets opgaver i artikel 66, stk. 1, i Kommissionens oprindelige forordningsforslag fra 2012[812] (svarende til den gældende artikel 70, stk. 1) var betydeligt mere kortfattet og overordnet, end det – efter de langvarige forhandlinger – blev tilfældet i den endelige udgave af forordningen. Detaljeringsgraden kan derfor ikke alene tilskrives rådets øgede aktivitetsområde.

8.4.3.3. Databeskyttelsesforordningens artikel 70, stk. 2 - 4

Af forordningens artikel 70, stk. 2, fremgår, at hvis Kommissionen anmoder Databeskyttelsesrådet om rådgivning, kan den (Kommissionen) fastsætte en frist under hensyntagen til, hvor meget den pågældende sag haster.

Efter forordningens artikel 70, stk. 3, fremsender Databeskyttelsesrådet sine udtalelser, retningslinjer, henstillinger og bedste praksis til Kommissionen og det udvalg, der er omhandlet i artikel 93[813], og offentliggør dem.

[812] KOM (2012) 11 endelig

[813] Før vedtagelsen af gennemførelsesretsakter skal Kommissionen høre et udvalg, der består af repræsentanter fra hvert EU-land, vedrørende det udkast, Kommissionen fremlægger, jf. Europa Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser. Databeskyttelsesforordningens artikel 93 omhandler dette udvalg.

Endelig følger det af forordningens artikel 70, stk. 4, at Databeskyttelsesrådet efter omstændighederne hører berørte parter og giver dem mulighed for at fremsætte bemærkninger inden for en rimelig frist. Databeskyttelsesrådet offentliggør med forbehold af artikel 76 om fortrolighed resultaterne af høringsproceduren.

8.4.3.4. Rapporter (artikel 71)

Efter forordningens artikel 71 udarbejder Databeskyttelsesrådet en årlig rapport om beskyttelse af fysiske personer i forbindelse med behandling i Unionen og, hvis det er relevant, i tredjelande og internationale organisationer. Rapporten offentliggøres og forelægges Europa-Parlamentet, Rådet og Kommissionen. Den årlige rapport skal omfatte en gennemgang af den praktiske anvendelse af de retningslinjer og henstillinger og den bedste praksis, der er omhandlet i artikel 70, stk. 1, litra l, og de bindende afgørelser, der er omhandlet i artikel 65.

Bestemmelsen videreføre i hovedtræk den ordning, der følger af direktivets artikel 30, stk. 6, hvorefter Artikel 29-gruppen udarbejder en årsberetning om situationen vedrørende beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger inden for Fællesskabet og i tredjelande. Denne beretning skal ligeledes forelægges for Europa-Parlamentet, Rådet og Kommissionen.

8.4.3.5. Afstemningsregler (artikel 72)

Det er fastsat i databeskyttelsesforordningens artikel 72, stk. 1, at Databeskyttelsesrådet træffer afgørelse med simpelt flertal blandt sine medlemmer, medmindre andet er fastsat i forordningen.

Der er tale om en videreførelse af retstilstanden efter direktivets artikel 29, stk. 3, hvorefter Artikel 29-gruppen træffer sine afgørelser med simpelt flertal blandt repræsentanterne for tilsynsmyndighederne (herunder EDPS).

Efter forordningens artikel 72, stk. 2, vedtager Databeskyttelsesrådet sin forretningsorden med et flertal på to tredjedele blandt sine medlemmer og tilrettelægger sin drift.

Som nævnt ovenfor er det på samme måde bestemt i direktivets artikel 29, stk. 6, at Artikel 29-gruppen selv fastsætter sin forretningsorden. Der stilles dog i direktivet ikke krav om, at forretningsordenen skal vedtages med et kvalificeret flertal.

8.4.3.6. Formandskab mv. (artikel 73-74)

8.4.3.6.1. Databeskyttelsesforordningens artikel 73

Rådet vælger efter forordningens artikel 73 med simpelt flertal en formand og to næstformænd blandt sine medlemmer. Embedsperioden for formanden og de to næstformænd er fem år med mulighed for forlængelse én gang.

Der er stort set tale om en kodificering af, hvad der allerede gælder i dag, hvor der foruden formanden – som efter direktivets artikel 29, stk. 4, vælges blandt medlemmerne af Artikel 29-gruppen, og hvis mandat kan fornyes – også vælges to næstformand, der efter udløbet af deres mandatperiode kan få denne fornyet, men kun én gang, jf. artikel 3 i gruppens nuværende forretningsorden.

Som noget nyt udvides formandskabets mandatperiode dog fra to år efter direktivets artikel 29, stk. 4, til fem år efter forordningen.

8.4.3.6.2. Databeskyttelsesforordningens artikel 74

Formanden har i medfør af forordningens artikel 74, stk. 1, til opgave at indkalde til møder i Databeskyttelsesrådet og udarbejde dagsordenen herfor (litra a), at underrette den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder om de afgørelser, der vedtages af Databeskyttelsesrådet i henhold til artikel 65 (litra b), og at sikre, at Databeskyttelsesrådets opgaver udføres rettidigt, navnlig i forbindelse med den sammenhængsmekanisme, der er omhandlet i artikel 63 (litra c).

Der er – bortset fra de i litra a nævnte opgaver – tale om opgaver, som udspringer af regler, der er nye med forordningen, hvorfor også formandens opgaver i den forbindelse er nye.

Det er i forordningens artikel 74, stk. 2, bestemt, at Databeskyttelsesrådet fastlægger fordelingen af opgaver mellem formanden og næstformændene i sin forretningsorden. Det må umiddelbart forventes, at rådet desuden fastsætter regler om mødefrekvens og -sted, arbejdssprog, quorum, afstemningsprocedure, dissens samt om nedsættelse af undergrupper og udpegning af rapporteurs mv.

8.4.3.7. Sekretariat (artikel 75)

Det fastslås i forordningens artikel 75, stk. 1 og 2, at Databeskyttelsesrådet har et sekretariat, som stilles til rådighed af Den Europæiske Tilsynsførende for Databeskyttelse, og at sekretariatet udelukkende udfører sine opgaver efter instruks fra formanden for Data-

beskyttelsesrådet. Til forskel herfra varetages sekretariatsopgaven for Artikel 29-gruppen af Kommissionen, jf. direktivets artikel 29, stk. 5.[814]

Efter forordningens artikel 75, stk. 3, skal det personale ved Den Europæiske Tilsynsførende for Databeskyttelse, der deltager i udførelsen af Databeskyttelsesrådets opgaver i henhold til forordningen, have særskilte rapporteringsveje i forhold til det personale, der deltager i udførelsen af opgaver, som EDPS har fået tildelt.

Endvidere følger det af forordningens artikel 75, stk. 4, at Databeskyttelsesrådet og EDPS udarbejder og offentliggør om nødvendigt et aftalememorandum til gennemførelse af denne artikel, som fastsætter vilkårene for deres samarbejde, og som gælder for det personale ved EDPS, der deltager i udførelsen af Databeskyttelsesrådets opgaver i henhold til forordningen.

Bestemmelserne om, at sekretariatet udelukkende udfører sine opgaver efter instruks fra rådets formand, og om de særskilte rapporteringsveje for de medarbejdere hos EDPS, der varetager opgaven, herunder muligheden for at udarbejde et aftalememorandum herom, understreger rådets uafhængighed.

På den anden side må bestemmelsen i forordningens artikel 75, stk. 4, om udarbejdelse af et aftalememorandum antages at begrænse rådets mulighed for ensidigt at fastsætte udfyldende regler om sekretariatets opgaver i sin forretningsorden.

Endelig er det i forordningens artikel 75, stk. 5 og 6, bestemt, at rådets sekretariat yder analytisk, administrativ og logistisk støtte til Databeskyttelsesrådet, herunder er sekretariatet ansvarligt for bl.a. forberedelse, udarbejdelse og offentliggørelse af udtalelser, afgørelser om bilæggelse af tvister mellem tilsynsmyndigheder og andre dokumenter, der vedtages af rådet.

8.4.3.8. Fortrolighed (artikel 76)

Forordningens artikel 76, stk. 1, fastslår, at Databeskyttelsesrådets drøftelser er fortrolige, hvis rådet vurderer, at det er nødvendigt, jf. dets forretningsorden.

Efter bestemmelsens stk. 2 er aktindsigt i dokumenter, der forelægges medlemmer af Databeskyttelsesrådet, eksperter og repræsentanter for tredjemand, omfattet af Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter.

[814] I praksis stiller også det tilsyn, der bestrider formandsposten for Artikel 29-gruppen, sekretariatsbistand til rådighed for gruppen.

Dette må antages at være en opretholdelse af status quo i forhold til Artikel 29-gruppen.[815]

8.4.4. Overvejelser

Som det fremgår af gennemgangen ovenfor, fastlægger forordningen Databeskyttelsesrådets opgaver mv. med udgangspunkt i databeskyttelsesdirektivets artikel 29 og 30 med tilføjelse af yderligere elementer, som bl.a. afspejler de nye opgaver, som rådet er givet med henblik på at fremme, at forordningen anvendes på en ensartet måde i medlemsstaterne.

Databeskyttelsesrådets status som en selvstædig juridisk person understreger den styrkelse og det statusløft i forhold til Artikel 29-gruppen, som rådet gives med forordningen, jf. også præambelbetragtning nr. 139.

Henset til den betydelige indflydelse, som Databeskyttelsesrådet må forventes at få på fortolkningen og udmøntningen af reglerne i forordningen, vil en meget aktiv deltagelse i rådet være en helt central opgave for Datatilsynet.

8.5. Databeskyttelsesrådets uafhængighed, artikel 69

8.5.1. Præsentation

I medfør af artikel 29 i det gældende databeskyttelsesdirektiv blev der nedsat en rådgivende og uafhængig gruppe (Artikel 29-gruppen) vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger.

Efter databeskyttelsesforordningens artikel 68 erstattes Artikel 29-gruppen med Det Europæiske Databeskyttelsesråd, som ifølge forordningens artikel 69 ligeledes skal være uafhængigt.

8.5.2. Gældende ret

Efter databeskyttelsesdirektivets artikel 29, stk. 2, er Artikel 29-gruppen uafhængig.

I databeskyttelsesdirektivets præambelbetragtning nr. 65 følger det om Artikel 29-gruppen, at den skal være fuldt uafhængig i udøvelsen af sine funktioner, og at den i kraft af denne uafhængighed skal rådgive Kommissionen og navnlig bidrage til, at de nationale regler, der vedtages til gennemførelse af databeskyttelsesdirektivet, anvendes ensartet.

[815] Peter Blume, Den nye persondataret (2016), s 158.

Artikel 29, stk. 2, og den nævnte præambelbetragtning stiller nogle nærmere krav til Artikel 29-gruppen, herunder dennes repræsentanter.

Hvad der overordnet skal forstås ved *fuld uafhængighed*, og hvad det generelt indebærer, er nærmere fastlagt af EU-Domstolen.

Ifølge EU-Domstolen indebærer fuld uafhængighed, at det pågældende organ ved udøvelsen af sine funktioner er unddraget enhver ydre påvirkning, hvad enten den er direkte eller indirekte.[816]

For nærmere om EU-Domstolens fortolkning af begrebet fuld uafhængighed henvises til afsnit 7.2. om tilsynsmyndighedernes uafhængighed.

Det skal hertil bemærkes, at kravet om fuld uafhængighed må antages at svare til uafhængighedskravet, som gælder for de nationale tilsynsmyndigheder. Der bør endvidere også sikres uafhængighed til Kommissionen.

Herudover må gruppens uafhængighed også anses for at være nærmere sikret ved, at det alene er gruppens repræsentanter fra medlemsstaternes uafhængige nationale tilsynsmyndigheder, der har stemmeret, når gruppen træffer afgørelse, jf. databeskyttelsesdirektivets artikel 29, stk. 3, at gruppen selv vælger sin formand, jf. artikel 29, stk. 4, og at gruppen selv fastsætter sin forretningsorden, jf. artikel 29, stk. 6.

8.5.3. Databeskyttelsesforordningen

Det følger af databeskyttelsesforordningens artikel 68, stk. 1, at der skal oprettes et europæisk databeskyttelsesråd (Databeskyttelsesrådet). Rådet skal ifølge forordningens præambelbetragtning nr. 139 erstatte Artikel 29-gruppen.[817]

Ifølge forordningens artikel 69, stk. 1, handler Databeskyttelsesrådet uafhængigt, når det udfører sine opgaver eller udøver sine beføjelser i henhold til artikel 70 og 71.

Endvidere følger det af artikel 69, stk. 2, at rådet ikke må søge eller modtage instrukser fra andre i forbindelse hermed, dog uden at det berører anmodninger fra Kommissionen som omhandlet i artikel 70, stk. 1, litra b, og stk. 2. Bestemmelsen i stk. 2 er på linje med EU-

[816] Bl.a. EU-Domstolens dom af 9. marts 2010 i sag C-518/07, Kommissionen mod Tyskland, præmis 18 ff.
[817] Se også Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), afsnit 3.4.7.3 i forslagets begrundelse smh. forslagets artikel 64.

Domstolens fortolkning af udtrykket "uafhængighed"[818] og må således anses at svare til, hvad der gælder for Artikel 29-gruppen i dag.

På linje hermed fremgår det af Kommissionens oprindelige forslag til forordningens artikel 69[819], at bestemmelsen understreger og præciserer Databeskyttelsesrådets uafhængighed.

Herudover er Databeskyttelsesrådets uafhængighed - svarende til hvad der i dag gælder for Artikel 29-gruppen - nærmere sikret ved, at dets repræsentanter i medfør af forordningens artikel 68, stk. 3, består af chefer fra uafhængige tilsynsmyndigheder, herunder fra Den Europæiske Tilsynsførende for Databeskyttelse (EDPS), eller deres repræsentanter, og at rådet vedtager sin egen forretningsorden.

For nærmere om kravene til de nationale tilsynsmyndigheders – og deres medlemmers – uafhængighed henvises til afsnit 7.2. EDPS' uafhængighed følger af forordning (EF) nr. 45/2001, kapitel V, særligt artikel 44.

8.5.4. Overvejelser

Bestemmelsen i forordningens artikel 69 regulerer Det Europæiske Databeskyttelsesråd, der er et EU-organ.

[818] Sag C-518/07, præmis 19.
[819] Afsnit 3.4.7.3 i forslagets begrundelse smh. forslagets artikel 65.

9. Forordningens kapitel VIII: Retsmidler, ansvar og sanktioner

9.1. Ret til at indgive klage, artikel 77

9.1.1. Præsentation

I databeskyttelsesforordningens artikel 77, stk. 1, fastsættes det, at enhver registreret har ret til at indgive klage til en tilsynsmyndighed, hvilket navnlig skal ske i den medlemsstat, hvor vedkommende har sit sædvanlige opholds- eller arbejdssted, eller hvor den pågældende overtrædelse har fundet sted, hvis den registrerede finder, at behandlingen af personoplysninger vedrørende vedkommende overtræder denne forordning.

Af databeskyttelsesforordningens artikel 77, stk. 2, følger det, at den tilsynsmyndighed, som klagen er indgivet til, underretter klageren om forløbet og resultatet af klagen, herunder om muligheden for anvendelse af retsmidler, jf. artikel 78.

9.1.2. Gældende ret

Det følger af databeskyttelsesdirektivets artikel 28, stk. 4, 1. afsnit, at enhver kan indgive en anmodning til tilsynsmyndigheden om beskyttelse af sine rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger. Det følger endvidere, at den pågældende underrettes om, hvorledes sagen følges op.

Det følger af direktivets artikel 28, stk. 4, 2. afsnit, at enhver især kan indgive en anmodning til tilsynsmyndighed om at få kontrolleret en behandlings lovlighed, når de nationale bestemmelser, der er truffet i henhold til artikel 13 i dette direktiv, finder anvendelse. Den pågældende underrettes i alle tilfælde om, at der er blevet foretaget en kontrol.

Det følger af direktivets præambelbetragtning nr. 62, at oprettelsen af en uafhængig tilsynsmyndighed i hver medlemsstat har afgørende betydning for beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger.

Det følger endvidere af direktivets præambelbetragtning nr. 63, at denne myndighed skal tildeles de fornødne beføjelser til at varetage denne opgave, herunder undersøgelses- og interventionsbeføjelser, navnlig når det drejer sig om klager, samt beføjelse til at indbringe sager for en retsinstans; myndigheden skal bidrage til at tilvejebringe gennemsigtighed i de databehandlinger, der udføres i den medlemsstat, hvorunder den hører.

Registerudvalget anførte i betænkning nr. 1345 om betydningen af direktivets artikel 28, stk. 4, at det første afsnit i stk. 4 omhandler den registreredes adgang til at rejse en sag.[820]

Det blev endvidere anført i betænkningen, at passagen "enhver kan ... især indgive en anmodning", jf. 2. afsnit, formentlig skal forstås på den måde, at man i direktivteksten har ønsket at understrege, at de personer (registrerede), som efter 1. afsnit skal kunne indgive en anmodning til tilsynsmyndigheden om beskyttelse i forbindelse med en behandlings lovlighed, især vil kunne gøre dette for at få kontrolleret en behandlings lovlighed, hvor der er særlig grund hertil. Dette er specielt vigtigt, når der i henhold til artikel 13 er sket undtagelse fra direktivets grundprincipper. Det synes endvidere overflødigt at pålægge myndigheden en egentlig pligt til at behandle klager fra ikke-registrerede, da det efter direktivet er tilsynsmyndighedens primære opgave at påse overholdelsen af lovgivningen. Myndigheden vil derfor i vidt omfang under alle omstændigheder behandle henvendelser fra ikke-registrerede, såfremt disse giver anledning til mistanke om, at der sker overtrædelser af lovgivningen. Det må på denne baggrund antages, at bestemmelsen alene medfører, at registrerede har adgang til at rejse en egentlig klagesag.[821]

Direktivets artikel 28, stk. 4, er udmøntet i national ret gennem persondatalovens § 40 og § 58, stk. 1.

Af persondatalovens § 40 følger det, at den registrerede kan klage til vedkommende tilsynsmyndighed over behandling af oplysninger vedrørende den pågældende. Denne bestemmelse har alene informativ karakter, og hvilken tilsynsmyndighed, der er kompetent, og hvilke regler der gælder for dennes virksomhed, må afgøres efter bestemmelserne i kapitel 16 og 17 om henholdsvis Datatilsynet og tilsynet med domstolene, der varetages af Domstolsstyrelsen.[822]

Af persondatalovens § 58, stk. 1, der også er baseret på direktivets artikel 28, stk. 4, følger det, at Datatilsynet af egen drift eller efter klage fra en registreret påser, at behandling finder sted i overensstemmelse med loven og regler udstedt i medfør af loven.

Det følger af bemærkningerne til persondataloven, at det foreslås, at Datatilsynet skal føre tilsyn med enhver behandling, der omfattes af loven, bortset fra behandlinger, der foretages for domstolene, og at Datatilsynet af egen drift eller efter klage fra en registreret person påser, at behandlingen finder sted i overensstemmelse med loven eller regler udstedt i med-

[820] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 359f.
[821] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 359f.
[822] Persondataloven med kommentarer (2015), s. 543f.

før af loven. Dette svarer til, hvad der fulgte af lov om offentlige myndigheders registre § 22, stk. 2, og lov om private registre § 22, stk. 1.[823]

Enhver registreret person eller virksomhed mv., som er beskyttet af loven, jf. § 1, kan (i overensstemmelse med det almindelige forvaltningsretlige partsbegreb) indgive en anmodning til Datatilsynet om beskyttelse af sine rettigheder efter loven, det vil typisk sige klage over en behandling, som vedkommende føler sig forurettet af. Tredjemand har ikke en ret til at klage til Datatilsynet med den følge, at tilsynet skal behandle sagen, men tilsynet kan og vil i sådanne tilfælde tage sagen og op af egen drift, hvis der vurderes at være anledning dertil.[824]

Det er Datatilsynets normale praksis ikke at iværksætte en selvstændig undersøgelse af, om der er sket lovlig behandling af personoplysninger i de tilfælde, hvor en sag allerede behandles af politiet. Tilsvarende vil normalt også gøre sig gældende, såfremt de forhold, der måtte kunne give anledning til en undersøgelse fra Datatilsynets side, allerede er genstand for undersøgelse af en anden (sær)tilsynsmyndighed på det pågældende område.[825]

Det følger af direktivets artikel 28, stk. 4, med *enhver kan*, at tilsynsmyndigheden, efter omstændighederne, vil kunne modtage klager fra registrerede i andre medlemsstater, ligesom registrerede i Danmark også vil kunne indgive klage til en tilsynsmyndighed i en anden medlemsstat, såfremt de mener, at deres rettigheder og frihedsrettigheder efter direktivet overtrædes af en dataansvarlig eller databehandler i en anden medlemsstat.

I sag C-230/14, Weltimmo, dom af 1. oktober 2015, havde et selskab, med hjemsted i Slovenien, administreret en internetside med annoncer for ejendomme beliggende i Ungarn, hvor annoncerne var gratis den første måned. Et betydeligt antal annoncører havde via e-mail anmodet om sletning af deres annoncer inden udløbet af den første måned samt anmodet om sletning af deres personlige oplysninger, hvilket selskabet ikke havde gjort. Selskabet havde derefter udstedt regninger til annoncørerne, der klagede til den ungarske tilsynsmyndighed.

EU-Domstolen anførte i præmis 44, at enhver person i henhold til artikel 28, stk. 4, i databeskyttelsesdirektivet kan indgive en anmodning om beskyttelse af sine rettigheder og frihedsrettigheder til tilsynsmyndigheden i forbindelse med behandling af personoplysninger.

[823] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.8.2. i de almindelige bemærkninger.
[824] Persondataloven med kommentarer (2015), s. 625.
[825] Persondataloven med kommentarer (2015), s. 626.

EU-Domstolen udtalte endvidere i præmis 54, at det således fremgår af artikel 28, stk. 6, i databeskyttelsesdirektivet, at en medlemsstats tilsynsmyndighed, som har modtaget en klage fra fysiske personer over behandlingen af personoplysninger om dem, på grundlag af direktivets artikel 28, stk. 4, kan undersøge denne klage uafhængigt af, hvilken ret der finder anvendelse og følgelig, selv om den ret, der finder anvendelse på behandlingen af de pågældende oplysninger, er en anden medlemsstats.

Der er ikke i persondataloven taget stilling til, hvordan tilsynsmyndigheden i forbindelse med en klagesag skal underrette den pågældende klager om, hvordan *sagen følges op*, eller om *at der er blevet foretaget en kontrol*.

Sådanne krav til tilsynsmyndigheden følger af de forvaltningsretlige regler, som tilsynet er underlagt. Vejledningspligten i medfør af forvaltningslovens § 7 medfører bl.a., at myndigheden er forpligtet til at udlevere eller beskrive allerede foreliggende oplysninger om ansøgningsprocedurer.[826] Derudover følger det af reglerne i forvaltningslovens kapitel 6, at en part skal underrettes, når myndigheden træffer en skriftlig afgørelse i sagen, herunder hvis klagen afvises.[827]

Det følger af en ombudsmandsudtalelse i en konkret sag om forlængelser af opholdstilladelser hos det daværende Udlændingeservice, at en offentlig myndighed skal give kvitteringsbreve og individuelle underretninger om sagsbehandlingstider. Heri må forstås, at der skal gives en ansøger løbende besked om, hvor lang tid det vil tage at behandle sagen.[828]

Derudover følger det af Justitsministeriets vejledning om forvaltningsloven, at hvis en forvaltningsmyndighed som følge af sagens karakter eller den almindelige sagsbehandlingstid for den pågældende myndighed ikke kan træffe afgørelse inden kortere tid efter sagens modtagelse, bør myndigheden give den, der er part i sagen, underretning om, hvorpå sagen beror og så vidt muligt oplysning om, hvornår myndigheden regner med, at afgørelsen kan foreligge.[829]

Endvidere følger det af vejledningen, at myndigheden endvidere bør give den, der er part i sagen, underretning, når behandlingen af den konkrete sag på grund af særlige omstændigheder vil tage længere tid end sædvanligt.[830]

---

[826] Hans Gammeltoft-Hansen m.fl., Forvaltningsretten, 2. udgave, 2002, s. 379.
[827] Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave (2013), s. 607 ff.
[828] FOB 2012-3, af 31. januar 2012.
[829] Vejledning nr. 11470 af 4. december 1986, om forvaltningsloven, punkt 206.
[830] Vejledning nr. 11470 af 4. december 1986, om forvaltningsloven, punkt 207.

Af Justitsministeriets cirkulæreskrivelse om mål for hurtig sagsbehandling mv. fremgår det bl.a., at borgeren under alle omstændigheder – hvor der ikke er fastsat særlige frister f.eks. i vejledninger – bør have et svar fra myndigheden inden 1 måned efter sagens modtagelse. Træffer myndigheden afgørelse i sagen inden 1 måned, udgøres svaret af afgørelsen. Er det ikke muligt at træffe afgørelse inden for denne frist, kan et foreløbigt svar til den pågældende bestå i, at myndigheden bekræfter at have modtaget sagen og oplyser, hvorpå sagen beror og så vidt muligt, hvornår en afgørelse kan forventes at foreligge.[831]

9.1.3. Databeskyttelsesforordningen

9.1.3.1. Databeskyttelsesforordningens artikel 77, stk. 1

Det følger af databeskyttelsesforordningens artikel 77, stk. 1, at uden at det berører andre administrative klageadgange eller adgang til domstolsprøvelse, har enhver registreret ret til at indgive klage til en tilsynsmyndighed, navnlig i den medlemsstat, hvor vedkommende har sit sædvanlige opholdssted eller sit arbejdssted, eller hvor den påståede overtrædelse har fundet sted, hvis den registrerede finder, at behandlingen af personoplysninger vedrørende vedkommende overtræder denne forordning.

Det følger bl.a. af præambelbetragtning nr. 141, at enhver registreret bør have ret til at indgive klage til en enkelt tilsynsmyndighed, navnlig i den medlemsstat, hvor vedkommende har sit sædvanlige opholdssted, og at undersøgelse af en klage bør foretages i det omfang, det er passende i det specifikke tilfælde, med forbehold af domstolskontrol.

Som nævnt ovenfor i afsnit 9.1.2., følger det allerede af direktivets artikel 28, stk. 4, som databeskyttelsesforordningens artikel 77, stk. 1, er baseret på, at registrerede har adgang til at rejse en egentlig klagesag.

Det følger af bestemmelsen, at enhver registreret har ret til at indgive klage, uden at det berører andre administrative klageadgange eller adgang til domstolsprøvelse. Heraf følger det, at retten til at indgive klage til en tilsynsmyndighed ikke afskærer den registrerede fra at benytte sig af andre muligheder, den registrerede måtte have *i medfør af national ret*, navnlig afskæres den registrerede ikke fra at anlægge sag ved domstolene. Det vil således være op til den registrerede at bestemme, hvorvidt der f.eks. ønskes indgivelse af en klage til tilsynsmyndigheden eller anlæggelse af en sag ved domstolene.

Retten til at indgive en klage modsvarer en pligt til at behandle klagen, hvilket fremgår af forordningens artikel 57, stk. 1, litra f, om at en af tilsynsmyndighedens opgaver er at behandle klager. Derudover følger det af forordningens artikel 57, stk. 2, at hver tilsynsmyn-

[831] Cirkulære nr. 73 af 4. juni 1997 om mål for hurtig sagsbehandling mv.

dighed letter indgivelsen af klager, jf. stk. 1, litra f, gennem foranstaltninger som f.eks. en klageformular, der også kan udfyldes elektronisk, uden at udelukke andre kommunikationsmidler. For en nærmere behandling af tilsynsmyndighedens opgaver henvises til afsnit 7.5. herom.

Derudover følger det af forordningens artikel 77, stk. 1, at den registreredes klageadgang, "navnlig [gælder] i den medlemsstat, hvor vedkommende har sit sædvanlige opholdssted eller sit arbejdssted, eller hvor den påståede overtrædelse har fundet sted". Bestemmelsen betyder således, at der kan være adgang til at indgive klage til tilsynsmyndigheder i andre medlemsstater.

Artikel 77 regulerer alene den registreredes ret til at indgive en klage, og det reguleres således ikke i bestemmelsen, hvilken tilsynsmyndighed der skal behandle klagen. Den tilsynsmyndighed, som klagen er indgivet til, vil dog i grænseoverskridende sager, i det mindste, være en berørt tilsynsmyndighed, jf artikel 4, nr. 22, litra c.

Det kan – såfremt der er tale om grænseoverskridende behandling, jf. artikel 4, nr. 23 – være nødvendigt at foretage en vurdering efter reglerne i forordningens artikel 56 af, hvilken medlemsstats tilsynsmyndighed, der skal være den ledende tilsynsmyndighed, og dermed have det overordnede ansvar for at koordinere samarbejdet mellem de forskellige medlemsstaters tilsynsmyndigheder efter proceduren i forordningens artikel 60. Denne procedure berører dog ikke den nationale tilsynsmyndigheds kompetence efter forordningens artikel 55, hvoraf det følger, at hver tilsynsmyndighed er kompetent på sin egen medlemsstats område. Derudover følger det af forordningens artikel 57, stk. 1, litra f, at en af tilsynsmyndighedens opgaver er at behandle klager fra registrerede.

9.1.3.2. Databeskyttelsesforordningens artikel 77, stk. 2

Det følger af databeskyttelsesforordningens artikel 77, stk. 2, at den tilsynsmyndighed, som klagen er indgivet til, underretter klageren om forløbet og resultatet af klagen, herunder om muligheden for anvendelse af retsmidler, jf. artikel 78.

Det følger bl.a. af præambelbetragtning nr. 141, at tilsynsmyndigheden bør underrette den registrerede om forløbet og resultatet af klagen inden for en rimelig frist. Hvis sagen kræver yderligere undersøgelse eller koordinering med en anden tilsynsmyndighed, bør den registrerede undervejs underrettes herom. For at lette indgivelsen af klager bør hver tilsynsmyndighed træffe foranstaltninger som f.eks. at tilbyde en klageformular, der også kan udfyldes elektronisk, uden at udelukke andre kommunikationsmidler.

Det følger af underretningspligten, at den tilsynsmyndighed, som klagen er indgivet til, som svar på den registreredes klage underretter denne om forløbet af klagen. Efter bestemmelsens ordlyd gør det ingen forskel, om den myndighed, som klagen blev indgivet til, er den tilsynsmyndighed, der har kompetence til at afgøre klagen. Det tilsyn, som har modtaget klagen, bibeholder efter artikel 77, stk. 2, kommunikationen med klageren, også i tilfælde, hvor det er et andet lands tilsynsmyndighed, der skal behandle klagen. Dette kunne f.eks. være, hvis klagen vedrører en dansk myndigheds behandlinger, men klagen er indgivet til det polske tilsyn.

Dermed kan der i ─ ikke-grænseoverskridende sager ─ opstå en situation, hvor en national tilsynsmyndighed ikke blot kan oversende en klage til behandling hos den kompetente tilsynsmyndighed og underrette klager herom.

Derudover må tilsynsmyndigheden underrette klageren, såfremt behandlingen af klagen kræver undersøgelser eller koordinering med en anden tilsynsmyndighed, som den registrerede ikke allerede er underrettet om. Endelig skal tilsynsmyndigheden underrette klageren om resultatet af klagen. I den særlige situation, hvor den danske tilsynsmyndighed er modtager af klagen, men ikke rette myndighed til at behandle denne, er der imidlertid tale om en ny forpligtelse.

Bestemmelsen indfører som noget nyt, at den registrerede skal underrettes om muligheden for anvendelse af retsmidler, hvilket skal ske senest samtidig med, at der oplyses om resultatet af klagen. Derudover præciserer bestemmelsen tilsynsmyndighedens underretningsforpligtelse over for den registrerede om forløbet og resultatet af klagen.

9.1.4. Overvejelser

Databeskyttelsesforordningens artikel 77, stk. 1, præciserer gældende ret ved at opliste de momenter, der har primær betydning for, hvilken medlemsstats tilsynsmyndighed en registreret har ret til at indgive klage til.

Databeskyttelsesforordningens artikel 77, stk. 2, indfører som noget nyt en forpligtelse for en tilsynsmyndighed, som har modtaget en klage, til at underrette om en række forhold, herunder om muligheden for anvendelse af retsmidler.

9.2. Adgang til effektive retsmidler over for en tilsynsmyndighed, artikel 78

9.2.1. Præsentation

Databeskyttelsesforordningens artikel 78, stk. 1-4, regulerer den registreredes adgang til effektive retsmidler (domstolsprøvelse) over for en tilsynsmyndighed, hvilken medlemsstat en sådan sag skal anlægges i, samt proceduren hvis sag anlægges på baggrund af en afgørelse, der er truffet af tilsynsmyndigheden efter en afgørelse eller udtalelse fra Databeskyttelsesrådet.

9.2.2. Gældende ret

9.2.2.1. Persondataloven og databeskyttelsesdirektivet

Det følger af databeskyttelsesdirektivets artikel 22, at medlemsstaterne fastsætter bestemmelser om, at enhver har ret til for en domstol at indbringe en klage over krænkelser af de rettigheder, der garanteres i henhold til de nationale love, der gælder for den pågældende behandling, uden at foregribe muligheden for at iværksætte administrativ klage, herunder for den tilsynsmyndighed, der er nævnt i artikel 28, inden forelæggelse for retsinstanser.

Derudover følger det af direktivets artikel 28, stk. 3, at afgørelser truffet af tilsynsmyndigheden, som går en involveret part imod, kan indbringes for en retsinstans.

Det følger af bemærkningerne til persondataloven, at der efter direktivets artikel 22 og 28, stk. 3, skal hjemles henholdsvis registrerede personer og dataansvarlige adgang til domstolsprøvelse.

Registerudvalget anførte i betænkning nr. 1345, at det følger af artikel 22, at medlemsstaterne skal fastsætte bestemmelser om, at enhver har ret til at indbringe en klage over krænkelser af de rettigheder, der garanteres i henhold til de nationale love, der gælder for den pågældende behandling for en domstol. Medlemsstaterne må ikke herved foregribe muligheden for at iværksætte administrativ klage, herunder for den tilsynsmyndighed, der er nævnt i artikel 28, inden forelæggelse for retsinstanserne.[832]

Derudover følger det af Registerudvalgets betænkning, at uanset anvendelsen af ordet "enhver" i direktivets artikel 22 må bestemmelsen antages at skulle forstås således, at der alene stilles krav om, at lovgivningen indrettes på en sådan måde, at den registrerede har mulighed for at indbringe spørgsmål om overtrædelser af lovgivningen for domstolene. Der kan med andre ord ikke af bestemmelsen antages at følge et krav om, at alle og enhver skal

[832] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 386.

have ret til at indbringe spørgsmål for domstolene (actio popularis). Dette fortolkningsresultat understøttes af de officielle engelske og franske oversættelser af direktivets artikel 22, hvoraf det klart fremgår, at bestemmelsen alene omhandler den registreredes ret til domstolsprøvelse.[833]

Endvidere følger det af Registerudvalgets betænkning, at der i den forbindelse tillige kan peges på, at bestemmelsen i artikel 28, stk. 3, sidste afsnit, også synes at forudsætte dette, idet bestemmelsen i modsat fald ikke vil have noget selvstændigt indhold. Af bestemmelsen i artikel 28, stk. 3, sidste afsnit, fremgår således, at afgørelser truffet af tilsynsmyndigheden, som går en involveret part imod, skal kunne indbringes for en retsinstans. Den selvstændige betydning af denne bestemmelse må - i lyset af artikel 22 - antages at være, at også dataansvarlige skal have adgang til domstolsprøvelse med hensyn til tilsynsmyndighedens afgørelser, udtalelser mv.[834]

Ydermere følger det af Registerudvalgets betænkning, at den adgang til domstolsprøvelse, som efter artikel 22 og artikel 28, stk. 3, sidste afsnit, skal hjemles henholdsvis registrerede personer og dataansvarlige, efter udvalgets opfattelse allerede er sikret i dansk ret. Af grundlovens § 63, stk. 1, følger således, at domstolene er berettiget til at påkende ethvert spørgsmål om overøvrighedsmyndighedens grænser. Denne mulighed for domstolsprøvelse vil bl.a. kunne udnyttes, såfremt Datatilsynet har behandlet en klage fra en registreret person. I givet fald vil den registrerede eller den dataansvarlige, som tilsynsmyndighedens afgørelse mv. måtte gå imod, kunne indbringe denne for domstolene.[835]

Endelig følger det af Registerudvalgets betænkning, at udvalget på denne baggrund ikke fandt, at der er behov for at indsætte en bestemmelse i lovgivningen om, at en *registreret* person kan indbringe spørgsmål om krænkelser af den pågældendes rettigheder i henhold til lovgivningen om behandling af personoplysninger for domstolene. Der fandtes endvidere ikke – under hensyntagen til det ovennævnte – at være behov for en bestemmelse om, at *dataansvarlige* kan indbringe tilsynsmyndighedens afgørelser, udtalelser mv. for domstolene.[836]

Det følger af persondatalovens § 61, at Datatilsynets afgørelser efter denne lov ikke kan indbringes for anden administrativ myndighed.

[833] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 386.
[834] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 386.
[835] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 386f.
[836] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 387.

Det følger af bemærkningerne til persondataloven, at bestemmelsen svarede til den tidligere retstilstand. Bestemmelsen er ikke til hinder for, at afgørelserne indbringes for Folketingets Ombudsmand.[837]

9.2.2.2. Domstolsprøvelse

Retsplejeloven fastsætter reglerne for, hvordan og hvornår den registrerede har adgang til domstolsprøvelse af, om dennes rettigheder er blevet krænket som følge af en overtrædelse af reglerne i persondataloven og databeskyttelsesdirektivet.

For at kunne anlægge en sag ved domstolene kræves det, at sagsøgeren har retlig interesse (søgsmålskompetence). Heri ligger, at sagsøgerens påstand skal være lovlig, aktuel og kunne bedømmes retligt, og at sagsøgeren skal have en konkret interesse i sagen.

Reglerne om og kravene til retlig interesse fremgår i vidt omfang af retspraksis, jf. f.eks. U.2013.3295 H, men kan dog også læses ud af enkelte bestemmelser i retsplejeloven. Det følger bl.a. af retsplejelovens § 252, stk. 1, at tredjemand, der har en retlig interesse i udfaldet af en sag, kan indtræde i sagen til støtte for en af parterne. Derudover følger det, at domstolene – såfremt partens påstand er uklar, og dermed ikke påviser partens retlige interesse – efter retsplejelovens § 339, stk. 1, har en vis mulighed for at afhjælpe uklare påstande ved at stille spørgsmål til den part, der har nedlagt påstanden.

Retsplejeloven fastsætter i kapitel 22 regler om stedlig kompetence (værnetingsregler), herunder hvor en offentlig myndighed kan sagsøges.

Det er udgangspunktet, at sager anlægges ved sagsøgtes hjemting, jf. retsplejelovens § 235, stk. 1. Det følger af retsplejelovens § 239, at regioner og kommuner har hjemting i den retskreds, hvor hovedkontoret ligger. Af retsplejelovens § 240, stk. 1, følger det, at staten har hjemting i den retskreds, hvor den myndighed, som stævnes på statens vegne, har kontor. Af samme bestemmelses stk. 2, følger det endvidere, at sager om prøvelse af afgørelser truffet af en central statslig myndighed anlægges ved sagsøgerens hjemting, hvis sagsøgeren har hjemting i Danmark.

Derudover følger det af retsplejelovens § 246, at sager mod personer, selskaber, foreninger, private institutioner og andre sammenslutninger, der ikke har hjemting i Danmark, kan anlægges her i landet, for så vidt nogen ret efter bestemmelserne i §§ 237, 238, stk. 2, 241, 242, 243 og 245 kan anses som værneting i sagen.

[837] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 61.

Det må følge modsætningsvist af retsplejelovens § 240, stk. 2, og af oplistningen i retsplejelovens § 246, at søgsmål mod danske offentlige myndigheder ikke kan anlægges i udlandet, og at søgsmål mod udenlandske offentlige myndigheder ikke kan anlægges i Danmark, når der er tale om udøvelse af offentligretlige beføjelser.

9.2.2.3. EU-retten

TEUF artikel 263 regulerer bl.a., hvornår der er direkte adgang til at få EU-Domstolen til at tage stilling til lovligheden af lovgivningsmæssige retsakter vedtaget af EU-institutionerne, der skal have virkning over for tredjemand.

For at få EU-Domstolen til at tage stilling til spørgsmålet kræves, ligesom efter dansk ret, at der er retlig interesse. Betingelserne er beskrevet i TEUF artikel 263, stk. 4, hvoraf det følger, at "enhver fysisk eller juridisk person kan på det grundlag, der er omhandlet i stk. 1 og 2, indbringe klage med henblik på prøvelse af retsakter, der er rettet til vedkommende, eller som berører denne umiddelbart og individuelt, samt af regelfastsættende retsakter, der berører vedkommende umiddelbart, og som ikke omfatter gennemførelsesforanstaltninger." Derudover fastsætter artikel 263, stk. 6, en to måneders frist for indgivelse af klager.

TEUF artikel 267 fastsætter reglerne for præjudicielle spørgsmål ved EU-Domstolen. Det er i udgangspunktet op til de nationale domstole – under nærmere fastsætte betingelser – at afgøre, hvorvidt EU-Domstolen bør anmodes om at tage stilling til præjudicielle spørgsmål. Betingelser for, hvornår nationale domstole skal stille præjudicielle spørgsmål afhænger af, hvorvidt der – efter national ret – er adgang til at appellere dommen. Såfremt der er mulighed for at appellere, *kan* den nationale ret stille eventuelle præjudicielle spørgsmål til EU-Domstolen. Såfremt der ikke er mulighed for at appellere, *skal* den nationale ret stille eventuelle præjudicielle spørgsmål til EU-Domstolen.

Chartret om grundlæggende rettigheder fastsætter en række grundlæggende rettigheder, friheder og principper, som medlemsstaterne skal respektere, når de gennemfører EU-ret. Artikel 47 i chartret vedrører bl.a. adgangen til *effektive retsmidler*. Det følger af chartrets artikel 47, stk. 1, at enhver, hvis rettigheder og friheder som sikret af EU-retten er blevet krænket, skal have adgang til effektive retsmidler for en domstol under overholdelse af betingelser, der er fastsat i denne artikel.

Formålet med chartrets artikel 47 er at sikre den effektive håndhævelse af EU-rettens materielle rettigheder hos EU-institutionerne og hos de nationale domstole ved at kræve, at der skal være tilgængelige retsmidler. Artikel 47 anvendes i henhold til de processuelle regler, der er fastsat i traktaterne. Det finder anvendelse over for EU's institutioner og medlemsstaterne, når de gennemfører fælleskabsretten, og gælder alle de rettigheder, der er sikret

ved EU-retten.[838] For at artikel 47 kan bringes i anvendelse, skal der af den grund foreligge en (påstået) krænkelse af en anden materiel rettighed. [839]

Chartrets artikel 47, stk. 1, kodificerer den i EU-retlig retspraksis udviklede pligt for medlemsstaterne til at tilvejebringe den nødvendige adgang til domstolsprøvelse for at sikre en effektiv retsbeskyttelse på de områder, der er omfattet af EU-retten.[840] De nationale domstole, der er omfattet af bestemmelsen, afgrænses på samme måde som de, der er berettigede til at stille præjudicielle spørgsmål til EU-Domstolen i medfør af TEUF artikel 267. Af chartrets artikel 47, stk. 1 følger det, at der for disse domstole skal være adgang til at få en stillingtagen til realiteten i sagen ved fortolkning og/eller anvendelse af gældende EU-ret og – i tilfælde af krænkelse – få en passende oprejsning.[841]

Chartrets artikel 47 kræver alene, at de nationale domstole giver borgerne adgang til at få en selvstændig prøvelse af endelige afgørelser og således ikke af procesledende beslutninger.[842]

I sag C-312/93, Peterbroeck, dom af 14. december 1995, var et selskab hjemmehørende i Holland blevet pålagt at betale skat som ikke-hjemmehørende i Belgien, hvilet betød, at selskabet skulle betale end højere skatteprocent, end der ville gælde for et belgisk selskab. EU-Domstolen tog i sagen stilling til, hvorvidt en national procesretlig bestemmelse, der afskar en national domstol fra at tage stilling til et nyt anbringende, der støttede sig på EU-retten, var forenelig med EU-retten.

EU-Domstolen anførte i præmis 12, at når der ikke er udstedt fællesskabsbestemmelser på området, tilkommer det hver enkelt medlemsstat i sin interne retsorden at udpege de kompetente retter og fastsætte de processuelle regler for sagsanlæg til sikring af beskyttelse af de rettigheder, som fællesskabsrettens direkte virkning medfører for borgerne. Disse processuelle regler må dog ikke være mindre gunstige end dem, der gælder for tilsvarende søgsmål på grundlag af national ret (ækvivalensprincippet), og de må heller ikke i praksis gøre det umuligt eller uforholdsmæssigt vanskeligt at udøve de rettigheder, der tillægges i henhold til Fællesskabets retsorden (effektivitetsprincippet).

---

[838] Den forklarende rapport til EU's Charter om grundlæggende rettigheder, EU-Tidende 2007/C 303/02, forklaring ad artikel 47.
[839] Jonas Christoffersen, EU's Charter om Grundlæggende Rettigheder med kommentarer, 1. udgave, 2014, s. 406.
[840] Den forklarende rapport til EU's Charter om grundlæggende rettigheder, EU-Tidende 2007/C 303/02, forklaring ad artikel 47.
[841] Jonas Christoffersen, EU's Charter om Grundlæggende Rettigheder med kommentarer, 1. udgave, 2014, s. 412.
[842] Jonas Christoffersen, EU's Charter om Grundlæggende Rettigheder med kommentarer, 1. udgave, 2014, s. 412.

EU-Domstolen anførte endvidere i præmis 14, at med henblik på anvendelsen af disse principper skal hvert enkelt tilfælde, hvor der opstår spørgsmål om, hvorvidt en national processuel bestemmelse gør det umuligt eller uforholdsmæssigt vanskeligt at anvende fællesskabsretten, bedømmes under hensyn til, hvilken stilling bestemmelsen indtager i den samlede procedure, herunder dens forløb og dens særlige kendetegn, for de forskellige nationale retsinstanser. Under denne synsvinkel skal der i givet fald tages hensyn til de principper, der ligger til grund for den nationale retspleje, bl.a. kontradiktionsprincippet, retssikkerhedsprincippet og princippet om en hensigtsmæssig sagsbehandling.

Medlemsstaterne har således processuel autonomi i fastsættelsen af de retsmidler og processuelle regler, når adgang til effektive retsmidler skal sikres i national ret til gennemførslen af krav baseret på EU-retten. Medlemsstaternes processuelle autonomi gælder kun på de områder, hvor der ikke er fastsat fælles EU-retlige regler, hvilket der f.eks. er i forkyndelsesforordningen og Bruxelles I-forordningen mv.[843]

I det omfang der ikke er fastsat fælles EU-retlige regler, f.eks. fordi det ikke følger af databeskyttelsesforordningen, vil det være national procesret – som i Danmark primært findes i retsplejeloven – der regulerer spørgsmålet om adgang til domstolene.

9.2.3. Databeskyttelsesforordningen

Det fremgår af Kommissionens forslag til databeskyttelsesforordningen, at den nuværende artikel 78 (artikel 74 i forslaget) vedrører retten til domstolsprøvelse af en tilsynsmyndigheds afgørelser, at den er baseret på den almindelige bestemmelse i artikel 28, stk. 3, i databeskyttelsesdirektivet, og at den specifikt omhandler et retsmiddel, der forpligter tilsynsmyndigheden til at reagere på en klage, og afklarer kompetencen for domstolene i den medlemsstat, hvor tilsynsmyndigheden er etableret.[844]

Det følger bl.a. af præambelbetragtning nr. 141, at enhver registreret bør have adgang til effektive retsmidler i overensstemmelse med artikel 47 i chartret, hvis den registrerede finder, at vedkommendes rettigheder i henhold til denne forordning er blevet krænket eller hvis tilsynsmyndigheden ikke reagerer på en klage, delvist eller helt afslår eller afviser en klage eller ikke handler, hvis handling er nødvendig for at beskytte den registreredes rettigheder.

Det følger af præambelbetragtning nr. 143, 1. afsnit, at enhver fysisk eller juridisk person har ret til at anlægge annullationssøgsmål til prøvelse af afgørelser fra Databeskyttelsesrå-

[843] Jonas Christoffersen, EU's Charter om Grundlæggende Rettigheder med kommentarer, 1. udgave, 2014, s. 413.
[844] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), afsnit 3.4.8.

det ved Domstolen på de betingelser, der er fastsat i artikel 263 i TEUF. De berørte tilsynsmyndigheder, som sådanne afgørelser er rettet til, skal, hvis de ønsker at anfægte afgørelserne, anlægge søgsmål inden for to måneder efter meddelelse af afgørelserne til dem i overensstemmelse med artikel 263 i TEUF. Når en dataansvarlig, databehandler eller klager er umiddelbart og individuelt berørt af Databeskyttelsesrådets afgørelser, kan disse anlægge annullationssøgsmål til prøvelse af disse afgørelser senest to måneder efter afgørelsernes offentliggørelse på Databeskyttelsesrådets hjemmeside i overensstemmelse med artikel 263 i TEUF.

Derudover følger det af betragtning nr. 143, at uden at dette berører denne ret i henhold til artikel 263 i TEUF, bør enhver fysisk eller juridisk person have adgang til effektive retsmidler ved den kompetente nationale domstol til prøvelse af en tilsynsmyndigheds afgørelse, som har retsvirkninger for denne person. En sådan afgørelse vedrører navnlig tilsynsmyndighedens udøvelse af undersøgelsesbeføjelser, korrigerende beføjelser og godkendelsesbeføjelser eller afslag eller afvisning af klager. Denne ret til adgang til effektive retsmidler omfatter dog ikke foranstaltninger truffet af tilsynsmyndigheder, der ikke er juridisk bindende, som f.eks. udtalelser eller rådgivning fra tilsynsmyndigheden. En sag mod en tilsynsmyndighed bør anlægges ved domstolene i den medlemsstat, hvor tilsynsmyndigheden er etableret, og bør føres i overensstemmelse med den pågældende medlemsstats retspleje. Det følger også, at disse domstole bør have fuld jurisdiktion, herunder jurisdiktion til at undersøge alle de faktiske og retlige omstændigheder, der er relevante for den tvist, som de får forelagt.

Det følger endvidere af præambelbetragtning nr. 143, 2. afsnit, at hvis en klage er blevet afslået eller afvist af en tilsynsmyndighed, kan klageren anlægge sag ved domstolene i samme medlemsstat. I forbindelse med domstolskontrol vedrørende anvendelsen af denne forordning kan eller i det tilfælde, der er omhandlet i artikel 267 i TEUF, skal de nationale domstole, som anser en afgørelse om spørgsmålet for nødvendig for at afsige dom, anmode Domstolen om en præjudiciel afgørelse om fortolkning af EU-retten, herunder denne forordning.

Det fremgår også af betragtning nr. 143, at hvis en afgørelse truffet af en tilsynsmyndighed, som gennemfører en afgørelse fra Databeskyttelsesrådet, anfægtes ved en national domstol, og gyldigheden af Databeskyttelsesrådets afgørelse er omtvistet, har den nationale domstol ikke beføjelse til at erklære Databeskyttelsesrådets afgørelse for ugyldig, men skal forelægge Domstolen spørgsmålet om gyldighed i henhold til artikel 267 i TEUF som fortolket af Domstolen, hvis den anser afgørelsen for ugyldig. En national domstol kan imidlertid ikke forelægge et spørgsmål om gyldigheden af Databeskyttelsesrådets afgørelse efter anmodning fra en fysisk eller juridisk person, der havde mulighed for at indbringe et

annullationssøgsmål til prøvelse af den pågældende afgørelse, navnlig hvis personen er umiddelbart og individuelt berørt af afgørelsen, men ikke havde gjort dette inden for fristen i henhold til artikel 263 i TEUF.

9.2.3.1. Databeskyttelsesforordningens artikel 78, stk. 1.

Det følger af databeskyttelsesforordningens artikel 78, stk. 1, at uden at det berører andre administrative eller udenretslige klageadgange, har *enhver fysisk eller juridisk person* ret til domstolsprøvelse af en juridisk bindende afgørelse truffet af en tilsynsmyndighed vedrørende vedkommende.

Som nævnt ovenfor, følger det af direktivets artikel 22, når det heri nævnes, uden at foregribe muligheden for at iværksætte administrativ klage, *herunder for den tilsynsmyndighed, der er nævnt i artikel 28,* at der også tænkes på andre typer af administrativ klage. Derudover følger det af direktivets artikel 28, at tilsynsmyndighedens afgørelser kan indbringes for en retsinstans.

Det fremgår af artikel 78, stk. 1, at enhver registreret har ret til domstolsprøvelse rettet mod tilsynet, *uden at det berører andre administrative eller udenretslige klageadgange.* Heraf følger det, at retten til at anlægge sag ved domstolene ikke påvirker den registreredes mulighed for at benytte sig af andre muligheder, den registreredes måtte have i medfør af national ret, navnlig afskæres den registrerede – ved at have ret til domstolsprøvelse – ikke fra at kunne klage til tilsynsmyndigheden.

Om kravet i forordningens artikel 78, stk. 1, om at der skal være tale om *en juridisk bindende afgørelse* følger det, at en medlemsstat ikke er forpligtet til at sikre adgang til domstolsprøvelse over for f.eks. tilsynsmyndighedens generelle udtalelser. Dette stemmer overens med forståelsen af chartrets artikel 47, hvorefter EU-retten alene kræver, at de nationale domstole giver borgerne adgang til selvstændig prøvelse af endelige afgørelser.

I og med, at der i gældende ret er en sådan adgang til domstolsprøvelse af Datatilsynets juridisk bindende afgørelser, der ikke berører andre administrative eller udenretslige klageadgange, må bestemmelsen i det hele anses for at være en videreførelse af gældende ret.

9.2.3.2. Databeskyttelsesforordningens artikel 78, stk. 2.

Det følger af databeskyttelsesforordningens artikel 78, stk. 2, at uden at det berører andre administrative eller udenretslige klageadgange, har den enkelte *registrerede* adgang til domstolsprøvelse rettet mod tilsynet, hvis den tilsynsmyndighed, der er kompetent i henhold til artikel 55 og 56, ikke behandler en klage eller undlader at underrette den registre-

rede om forløbet eller resultatet af en klage, der er indgivet i henhold til artikel 77, inden for tre måneder.

Artikel 78, stk. 2, præciserer under hvilke omstændigheder den registrerede skal have adgang til domstolsprøvelse over for en tilsynsmyndighed, når der allerede er indgivet en klage til Datatilsynet.

På baggrund af bestemmelsen kan den registrerede, såfremt det er gået mere end 3 måneder, siden den registrerede indgav en klage til tilsynet, forsøge at få dom for, at tilsynet skal behandle en klage eller underrette den registrerede om forløbet eller resultatet af en klage. Hvad der nærmere ligger heri må udfyldes i retspraksis.

9.2.3.3. Databeskyttelsesforordningens artikel 78, stk. 3.
Det følger af databeskyttelsesforordningens artikel 78, stk. 3, at en sag mod en tilsynsmyndighed anlægges ved en domstol i den medlemsstat, hvor tilsynsmyndigheden er etableret.

Det følger af præambelbetragtning nr. 143, at en sag mod en tilsynsmyndighed bør anlægges ved domstolene i den medlemsstat, hvor tilsynsmyndigheden er etableret, og bør føres i overensstemmelse med den pågældende medlemsstats retspleje. Disse domstole bør have fuld jurisdiktion, herunder jurisdiktion til at undersøge alle de faktiske og retlige omstændigheder, der er relevante for den tvist, som de får forelagt.

Betragtningen fastslår bl.a. – hvad der er det generelle udgangspunkt i EU-retten – at medlemsstaterne har national autonomi på det procesretlige område.

Det følger allerede af de generelle værnetingsregler i retsplejeloven, at sager mod offentlige myndigheder, herunder Datatilsynet, skal anlægges i Danmark, og af retsplejelovens § 240, stk. 2, at sager om prøvelse af afgørelser truffet af en central statslig myndighed, herunder f.eks. Datatilsynet, anlægges ved sagsøgerens hjemting, hvis sagsøgeren har hjemting i Danmark.

Medlemsstaterne opretter efter forordningens artikel 51 en eller flere uafhængige offentlige myndigheder, der er ansvarlige for at føre tilsyn med anvendelsen af denne forordning. Det må af den grund antages ikke at give anledning til tvivl om, hvilken medlemsstat en tilsynsmyndighed er etableret i.

Bestemmelsen præciserer, at sager mod tilsynsmyndigheden skal anlægges i den medlemsstat, hvor den er etableret.

9.2.3.4. Databeskyttelsesforordningens artikel 78, stk. 4.
Det følger af databeskyttelsesforordningens artikel 78, stk. 4, at hvis sag anlægges ved en national domstol mod en afgørelse fra en tilsynsmyndighed, der er truffet efter en udtalelse eller en afgørelse fra Databeskyttelsesrådet i forbindelse med sammenhængsmekanismen, fremsender tilsynsmyndigheden denne udtalelse eller afgørelse til domstolen.

For en nærmere behandling af Databeskyttelsesrådet og sammenhængsmekanismen henvises henholdsvis til afsnit 8.3. og 8.4. herom.

Det følger, som nævnt i ovenstående afsnit, af præambelbetragtning nr. 143, 2. afsnit, at en national domstol ikke har beføjelse til at erklære en afgørelse fra Databeskyttelsesrådet for ugyldig, men skal forelægge Domstolen spørgsmålet om gyldighed i henhold til artikel 267 i TEUF som fortolket af Domstolen, hvis den anser afgørelsen for ugyldig.

9.2.4. Overvejelser
Forordningens artikel 78, stk. 4, tilføjer – som noget nyt – en række processuelle krav til tilsynsmyndigheden i sager, hvor der anlægges sag mod denne ved domstolene, og hvor tilsynsmyndighedens afgørelser er truffet på baggrund af en udtalelse eller afgørelse fra Databeskyttelsesrådet i forbindelse med sammenhængsmekanismen.

9.3. Effektive retsmidler over for en dataansvarlig eller databehandler, artikel 79

9.3.1. Præsentation
Databeskyttelsesforordningens artikel 79, stk. 1 og 2, fastsætter, hvornår den registrerede har adgang til effektive retsmidler (domstolsprøvelse) over for en dataansvarlig eller en databehandler, og ved hvilken medlemsstat en sag skal anlægges.

Adgang til effektive retsmidler over for en dataansvarlig eller en databehandler følger af dansk rets almindelige betingelser for domstolsprøvelse.

9.3.2. Gældende ret
9.3.2.1. Persondataloven og databeskyttelsesdirektivet
Det følger af databeskyttelsesdirektivets artikel 22, at medlemsstaterne fastsætter bestemmelser om, at enhver har ret til for en domstol at indbringe en klage over krænkelser af de rettigheder, der garanteres i henhold til de nationale love, der gælder for den pågældende behandling, uden at foregribe muligheden for at iværksætte administrativ klage, herunder for den tilsynsmyndighed, der er nævnt i artikel 28, inden forelæggelse for retsinstanser.

Det følger bl.a. af direktivets præambelbetragtning nr. 55, at der i medlemsstaternes lovgivning skal gives adgang til at indbringe sagen for en retsinstans, hvis den dataansvarlige krænker en registrerets rettigheder.

Det fremgår af Registerudvalgets betænkninger nr. 1345, at denne mulighed for domstolsprøvelse bl.a. vil kunne udnyttes for behandlinger, som udføres for den offentlige forvaltning, der af den registrerede vil kunne indbringes for domstolene i medfør af grundlovens § 63, stk. 1. Med hensyn til behandlinger, som udføres for en privat dataansvarlig, bemærkes, at den registrerede efter retsplejelovens ordning vil kunne få prøvet spørgsmålet om behandlingernes forenelighed med lovgivningen, hvilket vil kunne ske ved et direkte søgsmål mod den private dataansvarlige. Også de afgørelser, som efter persondatalovens § 67, stk. 3, træffes af vedkommende dataansvarlige domstol, kan indbringes for en højere retsinstans.[845]

Derudover følger det af Registerudvalgets betænkning i forhold til spørgsmålet om domstolsprøvelse efter gældende ret, at der alene gælder et krav om, at den registrerede skal have mulighed for at anlægge sag mod en dataansvarlig ved domstolene (og dermed ikke en databehandler), og at denne ret til domstolsprøvelse allerede er sikret i dansk ret, hvorfor det ikke er nødvendigt med en bestemmelse herom.[846]

For en nærmere redegørelse af Registerudvalgets overvejelser om domstolsprøvelse henvises til afsnit 9.2. om adgang til effektive retsmidler over for en tilsynsmyndighed.

Det er centralt for begrebet databehandler i persondataloven, 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, jf. herved bl.a. reglen om erstatningsansvar i persondatalovens § 69.[847] Persondataloven forudsætter dermed, at det som udgangspunkt alene er den dataansvarlige, som den registrerede kan anlægge et civilretligt søgsmål mod ved domstolene med påstand om overtrædelser af lovens bestemmelser.

Databehandlere kan dog efter omstændighederne blive draget til ansvar efter reglerne om straf i persondatalovens § 70. Det kan bl.a. ske for overtrædelse af det af Datatilsynets i særlige tilfælde meddelte forbud eller påbud efter persondatalovens § 59, stk. 4.

[845] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 387.
[846] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 386f.
[847] Persondataloven med kommentarer (2015), s. 165.

Hvis det er en forudsætning mellem parterne, at den oprindelige dataansvarlige ikke længere kan råde over oplysninger, og at databehandleren selv kan disponere over de modtagne oplysninger til egne formål, er dataansvaret overgået til databehandleren, som betragtes som tredjemand og ny dataansvarlig. Dette kan have relevans for, hvorvidt den nye dataansvarlige af den registrerede kan sagsøges ved domstolene.[848]

Det følger af gennemgangen om søgsmålskompetence i afsnit 9.2. om adgang til effektive retsmidler over for en tilsynsmyndighed, at der for så vidt angår spørgsmålet om adgang til at anlægge en sag ved domstolene, som udgangspunkt ikke i dansk procesret skelnes mellem, hvorvidt der er tale om en retssag mod Datatilsynet eller en retssag mod en privat eller offentlig dataansvarlig. Sagsøgeren vil i alle tilfælde skulle påvise retlig interesse. Heri ligger, at sagsøgerens påstand skal være lovlig, aktuel, skal kunne bedømmes retligt, samt at sagsøgeren skal have en konkret interesse i sagen. Det følger dog af samme afsnit, at der for så vidt angår spørgsmålet om, hvor der kan anlægges sag – efter omstændighederne – kan være forskel mellem offentlige myndigheder og private virksomheder, i og med det følger af de danske værnetingsregler, at danske offentlige myndigheder skal sagsøges her i landet.

9.3.3. Databeskyttelsesforordningen

Kommissionen anførte i forslaget til forordningen fra 2012, at artikel 79 (artikel 75 i forslaget) omhandler retsmidler over for den dataansvarlige eller databehandleren og er baseret på artikel 22 i databeskyttelsesdirektivet, og at den giver sagsøger mulighed for at indbringe sagen for en domstol i den medlemsstat, hvor den sagsøgte er etableret, eller hvor den registrerede er bosiddende.[849]

Databeskyttelsesforordningens artikel 79 fastsætter reglerne for, hvornår en registreret har adgang til domstolsprøvelse over for en dataansvarlig eller en databehandler.

Det følger af præambelbetragtning nr. 147, at når denne forordning indeholder specifikke kompetenceregler, navnlig for så vidt angår sager om adgang til retsmidler, herunder erstatning, mod en dataansvarlig eller databehandler, bør de almindelige kompetenceregler i Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012 (Bruxelles I-forordningen) ikke berøre anvendelsen af sådanne specifikke regler.

For så vidt angår forståelsen af ”effektive retsmidler”, og for en nærmere behandling af chartrets artikel 47, henvises til afsnit 9.2. om adgang til effektive retsmidler over for en tilsynsmyndighed.

[848] Persondataloven med kommentarer (2015), s. 166.
[849] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), afsnit 3.4.8.

Der kan endvidere henvises til afsnit 9.6. om ret til erstatning efter artikel 82 og afsnit 9.4. om ret til repræsentation af registrerede efter artikel 80.

9.3.3.1. Databeskyttelsesforordningens artikel 79, stk. 1.

Det følger af databeskyttelsesforordningens artikel 79, stk. 1, at uden at det berører andre tilgængelige administrative eller udenretslige klageadgange, herunder retten til at indgive klage til en tilsynsmyndighed i henhold til artikel 77, skal den enkelte registrerede have adgang til effektive retsmidler, hvis vedkommende finder, at vedkommendes rettigheder i henhold til denne forordning er blevet krænket som følge af behandling af vedkommendes personoplysninger i strid med denne forordning.

Bestemmelsen fastsætter, at den registreredes adgang til domstolsprøvelse over for en dataansvarlig eller en databehandler, ikke må begrænses som følge af adgang til andre administrative eller udenretslige klageadgange.

Det følger allerede af direktivets artikel 22, at administrativ klageadgang ikke begrænser den registreredes mulighed for at anlægge sag ved domstolene, og at enhver har ret til for en domstol at indbringe en klage over krænkelser af de rettigheder, der garanteres i henhold til de nationale love, der gælder for den pågældende behandling.

Muligheden for at få domstolene til at tage stilling til en behandlings overensstemmelse med lovgivningen følger i dansk ret af grundlovens § 63, for så vidt angår en offentlig dataansvarlig, og forudsætningsvis af retsplejelovens § 255, stk. 1, for så vidt angår en privat dataansvarlig, hvoraf det fremgår, at hvo der er ret sagsøger eller sagvolder, afgøres efter lovgivningens almindelige regler.

Bestemmelsen i artikel 79, stk. 1, må således antages at være en videreførelse af gældende ret.

9.3.3.2. Databeskyttelsesforordningens artikel 79, stk. 2.

Det følger af databeskyttelsesforordningens artikel 79, stk. 2, at en sag mod en dataansvarlig eller en databehandler anlægges ved en domstol i den medlemsstat, hvor den dataansvarlige eller databehandleren er *etableret*. Alternativt kan en sådan sag anlægges ved en domstol i den medlemsstat, hvor den registrerede har sit *sædvanlige opholdssted*, medmindre den dataansvarlige eller databehandleren er en offentlig myndighed i en medlemsstat, der udøver sine offentligretlige beføjelser.

Forordningens artikel 79, stk. 2, regulerer således spørgsmålet om, hvor der er værneting. Det følger af bestemmelsen, at der både kan anlægges sager mod dataansvarlige *og* databe-

handlere. Dette er en udvidelse i forhold til, hvad der følger af databeskyttelsesdirektivet præambelbetragtning nr. 55, der alene nævner den dataansvarlige (og dermed ikke databehandleren), og persondatalovens § 69, der alene fastsætter erstatningsansvar for dataansvarlige.

Det er efter artikel 79, stk. 2, op til den registrerede at vurdere, hvorvidt en sag ønskes anlagt ved en domstol i den medlemsstat, hvor den dataansvarlige eller databehandleren er etableret, eller der, hvor den registrerede har sit sædvanlige opholdssted.

Præambelbetragtning nr. 145 gentager i vidt omfang, hvad der allerede følger af artikel 79, stk. 2. Af betragtningen følger det dog, at der kan anlægges sag i den medlemsstat, hvor den registrerede er *bosiddende,* og ikke, hvor den registrerede har sit *sædvanlige opholdssted*. Der antages imidlertid ikke at være forskel på de to begreber.

Den registrerede har dog ikke mulighed for at vælge, hvor en sag skal anlægges, hvis den dataansvarlige eller databehandleren er en offentlig myndighed, der udøver sine offentligretlige beføjelser. I dette tilfælde, vil der alene kunne anlægges sag i den medlemsstat, hvor den offentlige myndighed er etableret. Dette følger for dansk procesrets vedkommende allerede modsætningsvist af retsplejelovens § 240, stk. 2 og af oplistningen i § 246, at søgsmål mod danske offentlige myndigheder ikke kan anlægges i udlandet, og at søgsmål mod udenlandske offentlige myndigheder ikke kan anlægges i Danmark.

Udover, at der skal være tale om en offentlig myndighed, skal denne myndighed også udøve sine *offentligretlige beføjelser*, før der ikke vil kunne anlægges sag mod behandling foretaget af denne i den medlemsstat, hvor den registrerede har sit sædvanlige opholdssted. Det er ikke defineret i forordningen, hvad der konstituerer en offentligretlig beføjelse. Det vil være omfattet af bestemmelsen, når myndigheden træffer afgørelse og i øvrigt udøver faktisk forvaltningsvirksomhed på myndighedens område.

Det vil ikke være udøvelse af en offentligretlig beføjelse, når en myndighed træffer privatretlige dispositioner, som det kendes fra forvaltningslovens § 2, stk. 2, f.eks. når en offentlig myndighed indgår et kontraktforhold med en privat aktør eller ved aftaleretlige dispositioner i tilknytning til en medarbejders ansættelsesforhold.

9.3.4. Overvejelser

Forordningens artikel 79, stk. 2, udvider den registreredes adgang til at anlægge sag mod en databehandler. Derudover har den registrerede muligheden for at anlægge sag mod en privat dataansvarlig eller en privat databehandler samt en offentlig myndighed, der ikke

udøver sine offentligretlige beføjelser, der, hvor den registrerede har sit sædvanlige opholdssted, hvilket er en udvidelse i forhold til gældende ret.

9.4. Repræsentation af den registrerede, artikel 80

9.4.1. Præsentation

Databeskyttelsesforordningens artikel 80, stk. 1, giver – under nærmere omstændigheder – den registrerede ret til at lade sig repræsentere af andre.

I medfør af forordningens artikel 80, stk. 2, gives der mulighed for nationalt at udvide hovedparten af de i stk. 1 nævnte omstændigheder til også at gælde uafhængigt af en bemyndigelse fra den registrerede.

9.4.2. Gældende ret

Det følger af databeskyttelsesdirektivets artikel 28, stk. 4, at enhver, eventuelt repræsenteret ved en sammenslutning, kan indgive en anmodning til tilsynsmyndigheden om beskyttelse af sine rettigheder og frihedsrettigheder i forbindelse med behandlingen af personoplysninger.

Der ses ikke i forbindelse med udarbejdelsen af persondataloven eksplicit at være taget stilling til, om der – med eller uden bemyndigelse – skulle gives organer, organisationer eller sammenslutninger mulighed for at repræsentere registrerede ved indgivelse af klager eller anlæggelse af søgsmål ved domstolene.

Registerudvalget anførte dog i betænkning nr. 1345, for så vidt angår direktivets artikel 28, stk. 4, at bestemmelsen omhandler den registreredes adgang til at rejse en sag, og at det må antages, at bestemmelsen alene medfører, at registrerede har adgang til at rejse en egentlig klagesag.[850]

Derudover anførtes det i betænkningen, at den adgang til domstolsprøvelse, som efter artikel 22 og artikel 28, stk. 3, sidste afsnit, skal sikres henholdsvis registrerede personer og dataansvarlige, efter udvalgets opfattelse allerede er sikret i dansk ret.[851]

9.4.2.1. Den registreredes ret til at bemyndige andre til at repræsentere sig

For så vidt angår den registreredes adgang til at lade sig repræsentere af andre under klagesager til Datatilsynet, gælder der et almindeligt princip, hvorefter den, der kommer i for-

[850] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 360.
[851] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 386f.

bindelse med den offentlige forvaltning, i almindelighed kan vælge at lade sig repræsentere eller bistå af andre, medmindre væsentlige modhensyn kan anføres til støtte for at begrænse denne ret, andet følger af lovgivningen på det pågældende område eller følger af forholdets natur.[852] For så vidt angår afgørelsessager er dette princip kodificeret i forvaltningslovens § 8, stk. 1. Det følger af bemærkningerne til forvaltningsloven, at den myndighed, der behandler sagen, afgør, om den, der optræder som partsrepræsentant, skal fremlægge en skriftlig fuldmagt eller på anden måde godtgøre, at den pågældende kan optræde som repræsentant for parten. Myndigheden kan endvidere kræve, at parten medvirker personligt, når det er af betydning for sagens afgørelse.

For så vidt angår den registreredes adgang til at lade sig repræsentere af andre ved anlæggelse af søgsmål følger dette af dansk rets regler om mandatarer.

Retsplejerådet anførte i betænkning nr. 1468, at det følger af fast praksis, at en part i visse tilfælde kan repræsenteres af en mandatar i retssager. Mandataren er ikke part i sagen. Mandataren er heller ikke procesfuldmægtig for parten, men mandatarens stilling kan dog sammenlignes hermed. Mandataren kan føre sagen på partens vegne på samme måde som en procesfuldmægtig, og mandatarens optræden i sagen bygger på partens bemyndigelse, der når som helst kan tilbagekaldes.[853]

Det blev endvidere anført i betænkningen, at det efter forhistorien til retsplejelovens § 124 (der bl.a. fastsætter retten til, at foreninger mv. som mandatar må udføre retssager for deres medlemmer) næppe kan antages, at der hermed udtømmende er gjort op med juridiske personers mulighed for at optræde som mandatar. Langt de fleste mandatarer er ganske vist foreninger, der optræder som mandatar for et medlem inden for foreningens interesseområde. Samtidig er der imidlertid også et antal sager, hvor mandataren ikke er en forening (eller lignende), eller hvor en forening optræder som mandatar for andre end et af foreningens medlemmer, uden at det er blevet opfattet som en overtrædelse af retsplejelovens § 124, hvorved bemærkes, at overtrædelse af retsplejelovens § 124 er strafsanktioneret. Som nævnt forekommer det i meget vidt omfang i praksis, at en forening kan optræde som mandatar for et medlem i sager inden for foreningens interesseområde.[854]

Det blev ydermere anført i betænkningen, at der i praksis er tilfælde, hvor en forening optræder som mandatar for en udenlandsk part, som ikke er medlem af foreningen, men som er i en tilsvarende situation som foreningens medlemmer. Derudover er der tilfælde, hvor

[852] FOB 2001.514 og FOB 2002.480 og jf. Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave (2013), s. 295.
[853] Retsplejerådets betænkning 1468/2005 om reform af den civile retspleje IV, gruppesøgsmål mv., s. 66.
[854] Retsplejerådets betænkning 1468/2005 om reform af den civile retspleje IV, gruppesøgsmål mv., s. 67.

andre end foreninger fører en sag som mandatar. Bevæggrunde herfor har bl.a. været tilfælde, hvor sagen reelt, om end ikke formelt, har direkte betydning for mandataren, og tilfælde hvor mandataren er konkret involveret i sagen, uden at det dog fremgår, om den pågældende eksempelvis risikerer at pådrage sig et rådgiveransvar, hvis sagen tabes. Derudover har der i praksis været tilfælde, hvor mandataren alene har en generel interesse i sagen, og hvor mandataren for så vidt lige så godt kunne have optrådt som biintervenient eller måske i nogle tilfælde som hovedintervenient. Det er dog vanskeligt at sammenfatte, hvem der kan optræde som mandatar i hvilke situationer.[855]

Endelig blev det anført i betænkningen, at der på baggrund af betænkningens afsnit om mandatarer måske kan opstilles den regel, at en fysisk eller juridisk person kan optræde som mandatar i en retssag, når denne har en retlig interesse i udfaldet af sagen, svarende til kriteriet for, hvornår en person kan indtræde i sagen som biintervenient.[856]

Retten til at indtræde i en sag som biintervenient følger af retsplejelovens § 252. Heraf følger det af stk. 1, at tredjemand, der har en retlig interesse i udfaldet af en sag, kan indtræde i sagen til støtte for en af parterne. Det følger af bemærkningerne til retsplejeloven, at bestemmelsen skal forstås således, at det er overladt til domstolenes skøn i det enkelte tilfælde at tillade biintervention, når dette findes rimeligt og velbegrundet.

For så vidt angår retten til at modtage erstatning på vegne af en registreret reguleres dette i visse tilfælde af lov om juridisk rådgivning.[857] Det følger af lovens § 1, stk. 1, at loven finder anvendelse på enhver, der i erhvervsmæssigt øjemed driver virksomhed med rådgivning af overvejende juridisk karakter, når modtageren af rådgivningen (forbrugeren) hovedsagelig handler uden for sit erhverv. Det følger af bemærkningerne til loven, at rådgivning ydet af f.eks. fagforeninger og interesseorganisationer til deres medlemmer som udgangspunkt ikke er omfattet, idet denne rådgivning ikke anses for at være erhvervsmæssig, ligesom rådgivning i denne sammenhæng som oftest vil være et accessorisk led i den almindelige medlemsbetjening om forhold, der i bred forstand har sammenhæng med foreningens formål. I særlige tilfælde, hvor f.eks. en fagforening tager særskilt betaling for en juridisk rådgivning, kan denne rådgivning blive omfattet af loven.

Hvis rådgivning omfattes af lovens anvendelsesområde følger det af lovens § 2, stk. 6, at en person, der foretager juridisk rådgivning ikke må modtage betroede midler fra kunden eller på kundens vegne. Det følger af bemærkningerne til loven, at dette f.eks. gælder ved udbetaling af et erstatningsbeløb. Lovens § 2, stk. 6, blev indsat som følge af et ændrings-

[855] Retsplejerådets betænkning 1468/2005 om reform af den civile retspleje IV, gruppesøgsmål mv., s. 70.
[856] Retsplejerådets betænkning 1468/2005 om reform af den civile retspleje IV, gruppesøgsmål mv., s. 71.
[857] Lov nr. 419 om juridisk rådgivning af 9. maj 2006.

forslag til det oprindelige lovforslag, da det fandtes betænkeligt, at enhver, som i erhvervsmæssigt øjemed kunne drive virksomhed med juridisk rådgivning, kunne modtage betroede midler fra kunden eller på kundens vegne. Heraf fulgte det endvidere, at forbuddet mod at modtage betroede midler var grundet i en beskyttelse af den enkelte forbruger.[858]

Forbuddet mod juridiske rådgiveres håndtering af betroede midler bør også ses i sammenhæng med, at der er en tæt regulering af advokaters håndtering af betroede midler.[859] Den tætte regulering skyldes antageligvis dels, ligesom ved juridisk rådgivning, at advokater driver virksomhed i erhvervsmæssigt øjemed, og dels at der ofte kan være tale om høje beløb, mange forskellige klientkonti mv.

Såfremt en organisation mv., der ikke driver virksomhed i erhvervsmæssigt øjemed, af den registrerede er bemyndiget til at repræsentere denne som mandater i en retssag, vil der antageligvis ikke være det samme behov for at sikre, at eventuelle betroede midler ikke anvendes utilbørligt af den bemyndigede organisation mv.

I retspraksis er det, for så vidt angår fagforeninger, tilladt sådanne at håndtere eventuelle betroede midler, jf. f.eks. sagen U.2005.3037 Ø. I sagen gav den registrerede sin fagforening fuldmagt til at lade denne modtage erstatning på den registreredes vegne. Sagen vedrørte N og O, der begge var ansat i A Aps, der blev erklæret konkurs den 28. oktober 2004. I forbindelse med konkursen havde de begge underskrevet en fuldmagt til deres fagforening, F. Der var tale om standardfuldmagter afgivet på Lønmodtagernes Garantifonds, LG's, blanketter til brug for anmeldelse over for fonden, hvorefter F fik uigenkaldelig fuldmagt til at varetage deres interesser og modtage eventuelle udbetalinger.

Det antages på den baggrund, at der efter de almindelige fuldmagtsregler i dansk ret er mulighed for, at organisationer mv., som ikke omfattes af § 1, stk. 1, i lov om juridisk rådgivning, f.eks. fordi de ikke drives med et erhvervsmæssigt øjemed, kan modtage betroede midler fra en registreret ved udbetalingen af et erstatningsbeløb som følge af en retssag, hvor samme organisation har haft bemyndigelse til at repræsentere den registrerede.

[858] Betænkning afgivet af Retsudvalget den 6. april over forslag nr. L 65, FT 2005/06, fremsat 16. december 2005 til lov nr. 419 af 9. maj 2006 om juridisk rådgivning, bilag 18, bemærkningerne til nr. 4.
[859] Bekendtgørelse om godkendelse af vedtægt om advokaters pligter med hensyn til behandlingen af betroede midler, nr. 286 af 22. juni 1983 med senere ændringer, udstedt i medfør af retsplejelovens § 127.

9.4.2.2. Repræsentation af den registrerede uden bemyndigelse

For så vidt angår andres mulighed for på vegne af og uden bemyndigelse fra den registrerede at anlægge søgsmål ved domstolene, kendes fra dansk ret regler om gruppesøgsmål, som reguleres af retsplejelovens kapitel 23a.

Det fremgår af retsplejelovens § 254 b, stk. 1, nr. 7, at det bl.a. er en betingelse for at anlægge et gruppesøgsmål, at der kan udpeges en gruppere repræsentant. Denne gruppere repræsentant kan være en forening, en privat institution eller anden sammenslutning, når søgsmålet falder inden for rammerne af sammenslutningens formål, jf. retsplejelovens § 254 c, stk. 1, nr. 2.

Et gruppesøgsmål omfatter som udgangspunkt alene de medlemmer, som har tilmeldt sig, jf. retsplejelovens § 254 e, stk. 5. Dog kan retten såfremt gruppesøgsmål i medfør af retsplejelovens § 254 e, stk. 8, vedrører krav, hvor det er klart, at kravene på grund af deres ringe størrelse almindeligvis ikke kan forventes fremmet ved individuelle søgsmål, og hvor det må antages, at et gruppesøgsmål med tilmelding ikke vil være en hensigtsmæssig måde at behandle kravene på, efter anmodning fra gruppere repræsentanten bestemme, at gruppesøgsmålet skal omfatte de gruppemedlemmer, der ikke har frameldt sig gruppesøgsmålet. Retten fastsætter en frist for ved skriftlig meddelelse at framelde sig gruppesøgsmålet. Retten bestemmer, hvortil framelding skal ske. Retten kan undtagelsesvis tillade, at framelding sker efter fristens udløb, hvis særlige grunde taler for det.

Det følger af bemærkningerne til retsplejeloven, at betingelsen om kravenes ringe størrelse vil være opfyldt, hvis kravene enkeltvis angår så små værdier eller interesser, at den berettigede i almindelighed ikke kan forventes at anlægge individuel retssag om sit krav. Betingelsen bør normalt kun anses for at være opfyldt, hvis det enkelte krav ikke overstiger ca. 2.000 kr.

Derudover følger det af bemærkningerne til retsplejeloven om betingelsen om hensigtsmæssighed, at det beror på en samlet vurdering af den enkelte sags konkrete omstændigheder, herunder navnlig antallet af berørte, om et gruppesøgsmål med tilmelding vil være en hensigtsmæssig måde at behandle kravene på. Som et eksempel på tilfælde, hvor betingelserne for at behandle sagen som et gruppesøgsmål efter frameldingsmodellen vil kunne være opfyldt, kan nævnes sager om krav fra et stort antal abonnenter hos et teleselskab under påberåbelse af, at teleselskabet i en periode har opkrævet en højere takst end hjemlet ved standardvilkår og lovgivning, og hvor den enkelte abonnents tilbagebetalingskrav kun udgør nogle få hundrede kroner.

Det er alene offentlige myndigheder, der ved lov er bemyndiget til det, som kan udpeges som gruppere repræsentanter i et frameldingsgruppesøgsmål, jf. retsplejelovens § 254 c, stk. 2. Det er i øjeblikket kun forbrugerombudsmanden, der er givet en sådan bemyndigelse. Efter dansk ret er der ikke derudover givet adgang til, at organer, organisationer eller sammenslutninger kan indgive klage til Datatilsynet eller til at anlægge søgsmål ved domstolene uden en bemyndigelse fra den registrerede.

9.4.3. Databeskyttelsesforordningen

Det fremgår af Kommissionens forslag til databeskyttelsesforordningen, at den nuværende artikel 80 (daværende artikel 73) bl.a. angiver de organer, organisationer eller sammenslutninger, der kan indgive en klage på vegne af den registrerede eller uafhængigt af en registrerets klage, hvis der er tale om brud på persondatasikkerheden.[860] Derudover fremgår det af Kommissionens forslag til databeskyttelsesforordningen, at den nuværende artikel 80 (daværende artikel 76) bl.a. fastlægger fælles regler for retssager, herunder organers, organisationers eller sammenslutningers ret til at repræsentere registrerede for domstolene.[861]

9.4.3.1. Databeskyttelsesforordningens artikel 80, stk. 1

Det følger af databeskyttelsesforordningens artikel 80, stk. 1, at den registrerede har ret til at bemyndige et organ, en organisation eller en sammenslutning, der er etableret i overensstemmelse med en medlemsstats nationale ret, som ikke arbejder med gevinst for øje, hvis vedtægtsmæssige formål er af almen interesse, og som er aktiv på området for beskyttelse af registreredes rettigheder og frihedsrettigheder med hensyn til beskyttelse af deres personoplysninger, til på sine vegne at udøve de rettigheder, der er omhandlet i artikel 77, 78 og 79, og til, hvis det er fastsat i medlemsstaternes nationale ret, at udøve retten til at modtage erstatning som omhandlet i artikel 82 på sine vegne.

Præambelbetragtning nr. 142 er i vidt omfang enslydende med bestemmelsen. Dog nævner betragtningen, at det vedtægtsmæssige formål skal være i samfundets interesse, og at organet, organisationen eller sammenslutningen skal beskæftige sig med beskyttelse af personoplysninger. Denne sproglige forskel har antageligvis ingen selvstændig betydning.

Bestemmelsen giver således en registreret ret til at bemyndige en organisation mv. til på dennes vegne at indgive klage til tilsynsmyndigheden eller til at anlægge søgsmål ved domstolene mod en tilsynsmyndighed, en dataansvarlig eller en databehandler, såfremt den registreredes rettigheder eller frihedsrettigheder efter forordningens bestemmelser er blevet krænket.

[860] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), afsnit 3.4.8.
[861] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), afsnit 3.4.8.

Det følger af bestemmelsen, at der udover den registreredes bemyndigelse er en række betingelser, der skal være opfyldt, før en organisation mv. kan repræsentere den registrerede.

For det første kræves en etablering i overensstemmelse med en medlemsstats nationale ret. Af dette krav kan der imidlertid ikke udledes, at etableringen skal være sket i overensstemmelse med en bestemt medlemsstats nationale ret, f.eks. hvor tilsynsmyndigheden er beliggende, eller hvor der anlægges sag ved domstolene. Det må af den grund antageligvis være tilstrækkeligt, at etableringen er sket i overensstemmelse med en af medlemsstaternes nationale ret. En dansk organisation vil f.eks. i medfør af bestemmelsen kunne repræsentere en registreret i at anlægge sag ved de svenske domstole, såfremt de andre betingelser i bestemmelsen er opfyldt.

For det andet følger det, at organisationen mv. ikke må arbejde med gevinst for øje. Denne betingelse må kunne forstås i overensstemmelse med det at drive virksomhed i erhvervsmæssigt øjemed, jf. lov om juridisk rådgivning. Såfremt en organisation mv. falder ind under anvendelsesområdet i lov om juridisk rådgivning, fordi den driver virksomhed i erhvervsmæssigt øjemed, vil den antageligvis heller ikke opfylde betingelsen i artikel 80, stk. 1, om ikke at arbejde med gevinst for øje.

Det følger for det tredje, at det vedtægtsmæssige formål skal være af almen interesse. Heri må det, henset til, at bestemmelsen sigter til at sikre beskyttelse af de registreredes rettigheder og frihedsrettigheder, være tilstrækkeligt, at det ud fra organisationens mv. vedtægter kan udledes, at det er borgeres, samfundets, almenvellets eller lignende interesser, som søges fremmet.

Det følger endelig for det fjerde, at organisationen mv. skal være aktiv på området for beskyttelse af registreredes rettigheder og frihedsrettigheder med hensyn til beskyttelse af deres personoplysninger. Der vil her være tale om en indskrænkning i forhold til den tredje betingelse, i og med, at organisationen mv. tillige i et vist omfang skal beskæftige sig med personoplysninger. Heri kan imidlertid ikke udledes et krav om, at organisationen mv. ikke også må beskæftige sig med andre områder end beskyttelse af personoplysninger.

De fire betingelser, der er kumulative, må overordnet set skulle sikre, at det er den registreredes rettigheder, der varetages.

Artikel 80, stk. 1, har til formål at sikre beskyttelsen af den registreredes grundlæggende rettigheder og frihedsrettigheder. I lyset heraf, kan det ikke antages, at den registrerede på forordningens område alene kan give bemyndigelse under de i artikel 80, stk. 1, nævnte

omstændigheder, såfremt national ret i videre omfang tillader den registrerede at overlade bemyndigelse til at lade andre repræsentere sig. Forordningens artikel 80, stk. 1, må navnlig have til formål at sikre, at den registrerede under alle omstændigheder har en ret til at lade sig repræsentere under de i bestemmelsen nævnte omstændigheder.

Dette betyder, at den vide adgang, der i dansk ret gælder på det forvaltningsretlige område til at lade sig repræsentere af andre, ikke begrænses af forordningens artikel 80, stk. 1. En sådan begrænsning ville være en begrænsning af den effektive beskyttelse af den registreredes ret til at indgive en klage til tilsynsmyndigheden efter forordningens artikel 77.

På samme måde begrænses muligheden for den registrerede til at lade andre repræsentere sig ved anlæggelse af søgsmål ved domstolene antageligvis ikke af forordningens artikel 80, stk. 1.

Endelig følger det af artikel 80, stk. 1, at den registrerede kan bemyndige organisationer mv. til at udøve retten til at modtage erstatning på sine vegne som omhandlet i artikel 82, hvis dette er fastsat i medlemsstatens nationale ret. Det følger, at en registreret i en række situationer kan bemyndige en organisation mv. til at udøve retten til at modtage erstatning, hvilket den registrerede på samme måde også vil kunne for så vidt angår de rettigheder, der følger af forordningens artikler 77, 78 og 79.

9.4.3.2. Databeskyttelsesforordningens artikel 80, stk. 2

Det følger af forordningens artikel 80, stk. 2, at medlemsstaterne kan fastsætte, at ethvert organ, enhver organisation eller enhver sammenslutning, jf. denne artikels stk. 1, *uafhængigt* af en bemyndigelse fra den registrerede har ret til at indgive en klage i den pågældende medlemsstat til den tilsynsmyndighed, der er kompetent i henhold til artikel 77, og til at udøve de rettigheder, der er omhandlet i artikel 78 og 79, hvis den/det har grund til at formode, at den registreredes rettigheder i henhold til denne forordning er blevet krænket som følge af behandling.

Det er efter bestemmelsen op til den enkelte medlemsstat at tage stilling til, om der skal gives de i artikel 80, stk. 1, nævnte organisationer mv. mulighed for at indgive klage eller anlægge sag uafhængigt af en bemyndigelse fra den registrerede. Det følger ikke af bestemmelsen, om organisationen mv. forud for anlæggelse af søgsmål, skal kontakte den registrerede om, at dennes rettigheder efter organisationens mv. opfattelse er blevet krænket, og hvad organisationen mv. i den forbindelse agter at foretage sig. Selvom det ikke er et udtrykkeligt krav i forordningen, taler hensynet til den registrerede, herunder til at denne skal have mulighed for effektivt at udnytte sine rettigheder, for, at en organisation mv., der ønsker at anlægge et søgsmål på vegne af en registreret eller en større gruppe af registrere-

de bør underrette de registrerede, som klagen eller søgsmålet vedrører, herom. Af bestemmelsen kan imidlertid ikke udledes et krav om, at registrerede skal have haft mulighed for at foretage sig noget, herunder f.eks. mulighed for inden en frist at framelde sig søgsmålet. I det omfang, der bliver behandlet personoplysninger om den registrerede, vil organisationen mv. dog, i medfør af forordningens artikel 13 eller 14, skulle oplyse den registrerede om række forhold, herunder det formål, som oplysningerne behandles til.

For at bestemmelsen finder anvendelse kræves en formodning for, at den registreredes rettigheder i henhold til forordningen er blevet krænket som følge af behandling. Heri må antageligvis ligge et krav til organisationen mv. om, at denne kan kvalificere krænkelsen ved f.eks. at henvise til en bestemmelse i forordningen, som behandlingen efter organisationens mv. opfattelse overtræder.

9.4.4. Overvejelser

Forordningens artikel 80, stk. 1, giver i mindre grad end gældende dansk ret mulighed for, at den registrerede kan bemyndige en organisation mv. til at repræsentere sig ved indgivelse af klage til tilsynsmyndigheden eller ved anlæggelse af søgsmål ved domstolene. Artikel 80, stk. 1, antages ikke at begrænse den registreredes rettigheder til efter gældende dansk ret at bemyndige andre til at repræsentere sig, hvorfor gældende ret i det hele vil kunne videreføres.

Forordningens artikel 80, stk. 2, åbner mulighed for nationalt at give de nævnte organisationer mv. en adgang til at indgive klage eller anlægge søgsmål uden en bemyndigelse fra den registrerede. Hvis man fra dansk side fastsætter en sådan ret vil der, for så vidt angår klage til tilsynsmyndigheden, være tale om en nyskabelse i forhold til gældende ret. Derudover vil der, for så vidt angår anlæggelse af søgsmål ved domstolene, i al væsentlighed være tale om en nyskabelse i forhold til gældende ret.

9.5. Udsættelse af en sag, artikel 81

9.5.1. Præsentation

Databeskyttelsesforordningens artikel 81 fastsætter regler for, hvordan en domstol skal forholde sig, såfremt der verserer en sag om samme genstand ved en domstol i en anden medlemsstat.

9.5.2. Gældende ret

Der er ikke i databeskyttelsesdirektivet eller i persondataloven bestemmelser, der fastsætter, hvordan en domstol skal forholde sig, såfremt der verserer en sag om samme genstand ved en domstol i en anden medlemsstat.

Spørgsmålet om, hvordan danske domstole skal forholde sig, såfremt sager vedrørende krav, som er indbyrdes sammenhængende, verserer for retter i forskellige medlemsstater, er på det civil- og handelsretlige område reguleret af Bruxelles I-forordningen[862], som Danmark er omfattet af via en parallelaftale, jf. retsplejelovens § 247.

For så vidt angår retssager mod offentlige myndigheder henvises til afsnit 9.2. om adgang til effektive retsmidler over for en tilsynsmyndighed, hvor det bl.a. følger, at søgsmål mod offentlige danske myndigheder ikke kan anlægges i udlandet, når der er tale om udøvelse af offentligretlige beføjelser. Derfor opstår der ikke spørgsmål om verserende sager om samme genstand ved en domstol i en anden medlemsstat på det offentligretlige område.

Hvis en offentlig myndighed derimod udøver privatretlige beføjelser vil de samme regler, som der gælder for private, herunder efter omstændighederne Bruxelles I-forordningen, finde anvendelse.

Bruxelles I-forordningens artikel 30 angår tilfælde, hvor indbyrdes sammenhængende krav fremsættes for retter i forskellige medlemsstater. Stk. 1 giver mulighed for, at den senest anlagte sag udsættes, indtil den først anlagte sag er afgjort. Stk. 2 giver, under en række yderligere betingelser, mulighed for, at den senest anlagte sag afvises med henblik på, at kravet inddrages i den først anlagte sag. Stk. 3 definerer, hvad der forstås ved indbyrdes sammenhængende krav.[863]

Formålet med bestemmelsen er at undgå dobbeltbehandling af samme problemstilling og dermed undgå ressourcespild og risikoen for uforenelige afgørelse. Uforenelige afgørelser er skadelige for retsordenen, og udgør samtidig en hindring for dommes fri bevægelighed, idet anerkendelse og fuldbyrdelse kan nægtes på dette grundlag, jf. Bruxelles I-forordningens artikel 45, stk. 1, litra c og d.[864]

---

[862] Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012 af 12. december 2012 om retternes kompetence og om anerkendelse og fuldbyrdelse af retsafgørelser på det civil- og handelsretlige område (Bruxelles I-forordningen).
[863] Ketilbjørn Hertz, Bruxelles I-forordningen med kommentarer, 2. udgave, 2015, s. 375.
[864] Ketilbjørn Hertz, Bruxelles I-forordningen med kommentarer, 2. udgave, 2015, s. 375.

Bruxelles I-forordningens artikel 30 er fakultativ, og giver således domstole, hvor der ikke er anlagt sag først, en skønsmæssig mulighed for at udsætte eller – efter anmodning fra en part – afvise sager.

Det fremgår af Bruxelles I-forordningens artikel 30, stk. 1, at såfremt sager vedrørende krav, som er indbyrdes sammenhængende, verserer for retten i forskellige medlemsstater, kan enhver anden ret end den, ved hvilken sagen først er anlagt, udsætte sagen.

Udsættelse kan ske efter anmodning fra en part eller ex officio. Bestemmelsen indeholder ingen nærmere angivelse af, hvornår udsættelse bør ske, og retten har således et ret frit skøn over, om udsættelse bør ske eller ej.[865]

Derudover fremgår det af bestemmelsens stk. 2, at hvis det er konstateret, at der verserer sager i første instans, som nævnt i stk. 1, kan enhver anden ret også, efter anmodning fra en af parterne, erklære sig inkompetent. Det er dog en forudsætning, at den ret, hvor sagen først blev anlagt, har kompetence til at påkende de indbyrdes sammenhængende krav fra en anden ret, og at dens lovgivning tillader forening af kravene.

Betingelsen vedrørende kompetence er navnlig begrundet i, at en part ikke skal risikere, at sagen afvises i én medlemsstat med henblik på behandling i en anden medlemsstat, hvorefter sagen også afvises i den anden medlemsstat.[866] Om den modtagende domstol har kompetence, i sager omfattet af Bruxelles I-forordningens anvendelsesområde, reguleres af dennes kapitel II – dog ikke af artikel 30, der i udgangspunktet ikke er en kompetenceregel.

For så vidt angår spørgsmålet om forening af sager eller om samlet behandling af flere sager, der ikke verserer ved samme ret, følger dette efter dansk ret af retsplejelovens § 254, stk. 2.

Det fremgår af retsplejelovens § 254, stk. 2, 1. pkt., at retten efter anmodning fra en part, kan henvise en sag i 1. instans til behandling ved en anden ret, hvis sagen, efter indhentet udtalelse fra den anden ret, findes mest hensigtsmæssigt at kunne behandles i forbindelse med en anden sag, der verserer ved denne anden ret, jf. dog § 247, stk. 1.

Det fremgår af bestemmelsen, at henvisningen til en anden ret ikke kan ske på tværs af Bruxelles I-forordningen, Domskonventionens eller Luganokonventionens regler. Henvisningen af en sag, der hører under disse regelsæt, kan derfor kun ske, hvis der efter forord-

[865] Ketilbjørn Hertz, Bruxelles I-forordningen med kommentarer, 2. udgave, 2015, s. 377.
[866] Ketilbjørn Hertz, Bruxelles I-forordningen med kommentarer, 2. udgave, 2015, s. 378.

ningen eller konventionen er stedlig kompetence for sagen ved den ret, hvortil der ønskes henvist.[867]

For så vidt angår spørgsmålet om, hvordan den henvisende ret skal forholde sig i forhold til den udtalelse fra den modtagende ret, som skal indhentes, følger det, at en byret alene vil kunne henvise til landsret eller Sø- og Handelsretten, hvis det sker med denne rets tilslutning. Hvis en byret ønsker at henvise til en anden byret, følger det som udgangspunkt, at den modtagne byret bedre kan vurdere konsekvenser af en henvisning end den henvisende byret. Derfor bør en byret næppe henvise en sag til en anden byret, hvis den modtagende byret har modsat sig dette. Henvisning af en sag i 1. instans kan ske på tværs af retsplejelovens almindelige regler om stedlig og saglig kompetence.[868]

For så vidt angår tidspunktet for, hvornår denne henvisning bør ske, er der ikke fastsat regler, der regulerer dette. Fordelene ved samlet behandling af sagerne vil imidlertid være størst, hvis henvisning sker på et tidligt tidspunkt under sagen, og retten bør derfor ved udøvelsen af sit skøn over, om henvisning skal ske, alt andet lige være mere tilbøjelig til at imødekomme en anmodning om henvisning, når anmodningen er fremsat på et tidligt tidspunkt under sagen.[869]

Endelig fremgår det af Bruxelles I-forordningens artikel 30 stk. 3, at der, ved indbyrdes sammenhængende krav i artikel 30, forstås krav, der er så snævert forbundne, at det er ønskeligt at behandle og påkende dem samtidig for at undgå uforenelige afgørelser i tilfælde af, at kravene blev påkendt hver for sig.

I Bruxelles I-forordningens artikel 30, stk. 3, skal uforenelige afgørelser underlægges en vid fortolkning, hvor det nærmere må forstås som modstridende afgørelser. Dette beror på, at artikel 30 skal fremme et hensigtsmæssigt samarbejde mellem retterne i forskellige medlemsstater, hvorfor den bør gives et vidt anvendelsesområde.[870]

Når det i forbindelse med anvendelsen af Bruxelles I-forordningens artikel 30 skal afgøres, hvornår en sag skal anses for anlagt, følger dette af Bruxelles I-forordningens artikel 32.

---

[867] Forslag nr. 41 fremsat 10. oktober 2006, FT 2006/07, til lov om ændring af retsplejeloven og forskellige andre love (Gruppesøgsmål mv.), de specielle bemærkninger til nr. 8 og 9 (§ 254).
[868] Bernhard Gomard m.fl., Retsplejeloven med kommentarer, bind I, 9. udgave, 2013, s. 594.
[869] Forslag nr. 41 fremsat 10. oktober 2006 til lov om ændring af retsplejeloven og forskellige andre love (Gruppesøgsmål mv.), de specielle bemærkninger til nr. 8 og 9 (§ 254).
[870] Ketilbjørn Hertz, Bruxelles I-forordningen med kommentarer, 2. udgave, 2015, s. 376.

9.5.3. Databeskyttelsesforordningen

Det følger af Kommissionens forslag til databeskyttelsesforordningen, at den nuværende artikel 81 (artikel 76 i forslaget) bl.a. fastlægger fælles regler for information af domstolene om parallelle sager i en anden medlemsstat, og domstolenes mulighed for at udsætte verserende sager i sådanne tilfælde.[871]

Det fremgår af præambelbetragtning nr. 147, at når denne forordning indeholder specifikke kompetenceregler, navnlig for så vidt angår sager om adgang til retsmidler, herunder erstatning, mod en dataansvarlig eller databehandler, bør de almindelige kompetenceregler i Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012 (Bruxelles I-forordningen) ikke berøre anvendelsen af sådanne specifikke regler.

Derudover fremgår det af præambelbetragtning nr. 144, at hvis en domstol, for hvilken der indbringes en sag til prøvelse af en afgørelse truffet af en tilsynsmyndighed, har grund til at tro, at en sag vedrørende samme behandling, f.eks. med samme genstand for så vidt angår behandling udført af den samme dataansvarlige eller databehandler, eller som hviler på samme grundlag, anlægges ved en kompetent domstol i en anden medlemsstat, bør den kontakte den pågældende domstol for at bekræfte eksistensen af sådanne relaterede sager.

Det fremgår endvidere af samme betragtning, at hvis der verserer relaterede sager for en domstol i en anden medlemsstat, kan enhver anden domstol end den, ved hvilken sagen først er anlagt, udsætte sagen. Domstolen kan også – efter begæring fra en af parterne – erklære sig inkompetent til fordel for den domstol, ved hvilken sagen først er anlagt, forudsat at denne domstol har kompetence til at behandle den pågældende sag, og forening af sådanne relaterede sager er tilladt i henhold til dens lovgivning.

Endelig fremgår det af samme betragtning, at sager anses for at være relaterede, når de er så snævert forbundne, at det er ønskeligt at behandle og påkende dem samtidig for at undgå risiko for uforenelige afgørelser som følge af, at de blev påkendt hver for sig.

9.5.3.1. Databeskyttelsesforordningens artikel 81, stk. 1

Det fremgår af databeskyttelsesforordningens artikel 81, stk. 1, at hvis en kompetent domstol i en medlemsstat har oplysninger om, at der verserer en sag vedrørende samme genstand for så vidt angår behandling foretaget af den samme dataansvarlige eller databehandler ved en domstol i en anden medlemsstat, skal den rette henvendelse til pågældende domstol i den anden medlemsstat for at bekræfte eksistensen af en sådan sag.

[871] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig, afsnit 3.4.8.

Det følger af bestemmelsen, at domstolen skal have oplysning om, at der verserer en sag med samme genstand ved en domstol i en anden medlemsstat. Det er ikke i bestemmelsen afgrænset, hvem der kan oplyse domstolen om, at der verserer en sådan sag. En sådan oplysning antages i praksis primært at komme fra en domstol i en anden medlemsstat, fra den registrerede, der har anlagt søgsmålet, eller fra den sagsøgte dataansvarlige eller databehandler. Ud fra bestemmelsen kan der ikke udledes en *pligt* for domstolen til at foretage en *selvstændig undersøgelse* af, hvorvidt der verserer sager, som vil være omfattet af bestemmelsen. Domstolen vil dog, såfremt den har en sådan oplysning, være forpligtet til at rette henvendelse til den pågældende domstol for at bekræfte eksistensen af en sådan sag.

Domstolens forpligtelse til at rette henvendelse efter forordningens artikel 81, stk. 1, følger ikke direkte af gældende ret, og må på den baggrund anses for at være en nyskabelse i forhold til gældende ret.

9.5.3.2. Databeskyttelsesforordningens artikel 81, stk. 2

Det fremgår af databeskyttelsesforordningens artikel 81, stk. 2, at hvis der verserer en sag vedrørende samme genstand for så vidt angår behandling foretaget af den samme dataansvarlige eller databehandler ved en domstol i en anden medlemsstat, kan enhver anden kompetent domstol end den, ved hvilken sagen først er anlagt, udsætte sagen.

Det følger allerede i dag – på det civil- og handelsretlige område – af den fastlagte procedure i Bruxelles I-forordningens artikel 30, stk. 1, at en domstol kan vælge at udsætte en sag, hvis domstolen, som følge af en anmodning fra en part eller ex officio, har en oplysning om, at der verserer en sag ved en domstol i en anden medlemsstat vedrørende krav, som er indbyrdes sammenhængende med kravene i den sag, der verserer for den første domstol.

Såfremt domstolen vælger at udsætte sagen efter forordningens artikel 81, stk. 2, må domstolen herefter tage stilling til, om domstolen kan erklære sig inkompetent efter reglerne i forordningens artikel 81, stk. 3.

Domstolenes mulighed for at udsætte en sag, når en sag vedrørende samme genstand for så vidt angår behandling foretaget af den samme dataansvarlige eller databehandler verserer ved en domstol i en anden medlemsstat, må i det hele anses for at være en videreførelse af gældende ret.

9.5.3.3. Databeskyttelsesforordningens artikel 81, stk. 3

Databeskyttelsesforordningens artikel 81, stk. 3, fastsætter en mulighed for, at en domstol – under nærmere fastlagte omstændigheder - kan erklære sig inkompetent.

Det følger af bestemmelsen, at hvis denne sag verserer ved en domstol i en anden medlemsstat, kan enhver anden domstol - hvis en af sagens parter anmoder om det – også erklære sig inkompetent til fordel for den domstol, hvor sagen først er anlagt. Dette kræver dog, at den domstol, hvor sagen først er anlagt, har kompetence til at behandle de pågældende sager, og at forening af sagerne er tilladt i henhold til dens lovgivning. Derudover fremgår det af bestemmelsen, at den domstol, hvor sagen først er anlagt, ikke kan erklære sig inkompetent.

Med *denne sag* må der, i og med, at artikel 81, stk. 1 og 2, vedrører det forhold, at der verserer sager med samme genstand ved domstolene i flere medlemsstater, også i artikel 81, stk. 3, være tale om, at sagen har samme genstand. Bestemmelsens ordlyd, hvorved domstolen "også" kan erklære sig inkompetent taler for, at det er sådan bestemmelsen må forstås.

Bestemmelsens ordlyd er derudover i al væsentlighed i overensstemmelse med ordlyden af Bruxelles I-forordningens artikel 30, stk. 2.

Det følger af bestemmelsen, at enhver anden domstol end den, hvor sagen først er anlagt, har mulighed for at erklære sig inkompetent, såfremt en række betingelser er opfyldt. For det første kræves det, at sagen skal versere ved første instans. For det andet kræves, at en af parterne skal anmode domstolen herom. For det tredje skal den domstol, hvor sagen først er anlagt have kompetence til at behandle de pågældende sager. Endelig skal forening af sagerne være tilladt i henhold til lovgivningen i den stat, hvor den første domstol er beliggende. Det kræves således ikke i bestemmelsen, at forening af sagerne skal være tilladt i henhold til lovgivningen i den medlemsstat, som den anmodede domstol er underlagt.

De fire betingelser er kumulative og skal således være opfyldt, før de pågældende sager kan behandles samlet. Kravene må i praksis få den betydning, at enhver senere domstol først må anmode den domstol, hvor sagen først er anlagt, om at tage stilling til spørgsmålet om kompetence, og om at vurdere om forening af sagerne vil være tilladt i henhold til dens lovgivning. Den anmodende domstol må udsætte sagen, indtil der er taget stilling hertil, jf. artikel 81, stk. 2. Vurderer den første domstol, at den har kompetence til at behandle de pågældende sager samlet, og at forening er tilladt efter dens lovgivning, kan den anmodende domstol, i stedet for at udsætte sagen efter artikel 81, stk. 2, vælge at erklære sig inkompetent efter artikel 81, stk. 3. Hvis domstolen vælger at erklære sig inkompetent, skal de pågældende sager behandles samlet ved den første domstol, og den anmodende domstol vil ikke på et senere tidspunkt skulle tage stilling til sagen.

Hvad angår betingelsen om, at forening af sager skal være tilladt i henhold til lovgivningen i den medlemsstat, som den anmodede domstol er underlagt bemærkes det, at dette for dansk ret – i langt de fleste tilfælde – følger af reglerne i retsplejelovens § 254, stk. 2.

Spørgsmålet om, hvor en sag mod en dataansvarlig eller databehandler kan anlægges, og altså hvornår en domstol efter forordningens bestemmelser har kompetence til at behandle en sag, er reguleret af forordningens artikel 79, stk. 2, hvoraf det bl.a. fremgår, at en sag mod en privat dataansvarlig eller databehandler anlægges, hvor denne er etableret, eller hvor den registrerede har sit sædvanlige opholdssted.

9.5.4. Overvejelser

Domstolens forpligtelse til at rette henvendelse efter forordningens artikel 81, stk. 1, følger ikke direkte af gældende ret og må på den baggrund anses for at være en nyskabelse i forhold til gældende ret.

Domstolenes mulighed for at udsætte en sag efter forordningens artikel 81, stk. 2, og for at erklære sig inkompetent efter forordningens artikel 81, stk. 3, følger allerede af Bruxelles I-forordningens artikel 30, stk. 1 og stk. 2, og må i det hele anses for at være en videreførelse af gældende ret.

9.6. Ret til erstatning og erstatningsansvar, artikel 82

9.6.1. Præsentation

Databeskyttelsesforordningens artikel 82, stk. 1 og 2, fastsætter regler om retten til erstatning og om dataansvarliges og databehandleres erstatningsansvar.

Derudover fastsætter forordningens artikel 82, stk. 3-6, et præsumptionsansvar (culpa med omvendt bevisbyrde), solidarisk hæftelse, såfremt der er mere end én dataansvarlig eller databehandler, hvornår udbetalt erstatning kan kræves tilbagebetalt fra andre involverede (regression), samt hvor en erstatningssag skal anlægges.

9.6.2. Gældende ret

9.6.2.1. Databeskyttelsesdirektivet

Det følger af artikel 23, stk. 1, i databeskyttelsesdirektivets, at medlemsstaterne fastsætter regler om, at enhver, som har lidt skade, som følge af en ulovlig behandling eller anden behandling, der er uforenelig med de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, har ret til erstatning for den forvoldte skade fra den dataansvarlige.

Det følger af direktivets artikel 23, stk. 2, at den dataansvarlige helt eller delvist kan fritages for erstatningsansvar for skade, hvis han beviser, at han ikke er skyld i den begivenhed, der medførte skaden.

Af direktivets præambelbetragtning nr. 55 følger det, at personer, som lider skade som følge af en ulovlig behandling, skal have ret til erstatning fra den dataansvarlige, og at der skal iværksættes sanktioner over for såvel privatretlige som offentlige personer, der overtræder nationale bestemmelser vedtaget med henblik på gennemførelsen af dette direktiv.

9.6.2.2. EU-retlig retspraksis

EU-Domstolen har i en række sager fortolket begrebet "skade", herunder hvorvidt og i hvilke situationer begrebet, foruden økonomisk skade, også omfatter ikke-økonomisk skade.

I sag C-168/00, Leitner, dom af 12. marts 2002, havde en person købt en pakkerejse og blev i forbindelse med afholdelsen af denne syg med symptomer på salmonellaforgiftning.

EU-Domstolen udtalte i præmis 19, at [pakkerejse]direktivets[872] artikel 5, stk. 2, 1. afsnit, forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at rejsearrangøren erstatter "de skader, der påføres forbrugeren som følge af manglende eller mangelfuld opfyldelse af kontrakten".

EU-Domstolen udtalte endvidere i præmis 21, at det imidlertid står fast, at hvis der inden for pakkerejseområdet i visse medlemsstater var en forpligtelse til at erstatte ikke-økonomiske skader, og der ikke var en sådan forpligtelse i andre medlemsstater, ville dette medføre væsentlige konkurrenceforvridninger, da der – som Kommissionen også anførte i sagen – ofte konstateres ikke-økonomiske skader inden for dette område.

EU-Domstolen udtalte endelig i præmis 23 bl.a., at selv om artikel 5, stk. 2, 1. afsnit, begrænser sig til generelt at henvise til begrebet "skader", skal det bemærkes, at idet artikel 5, stk. 2, 4. afsnit, fastsætter muligheden for, at medlemsstaterne for så vidt angår andre skader end legemlige skader kan tillade, at erstatningen begrænses i henhold til kontrakten under forudsætning af, at begrænsningen ikke er urimelig, anerkender direktivet stiltiende et krav på godtgørelse for andre skader end legemlige skader, herunder ikke-økonomisk skade.

[872] Rådets direktiv af 13. juni 1990 om pakkerejser, herunder pakkeferier og pakketure (90/314/EØF).

I sag C-277/12, Drozdovs, dom af 24. oktober 2013, omkom sagsøgers forældre i et trafikuheld, hvilket medførte at sagsøger anmodede forsikringsselskabets om og her fik udbetalt en erstatning, hvis størrelse sagsøger var uenig i.

EU-Domstolen udtalte i præmis 38, at det, henset til de forskellige sprogversioner af andet direktivs[873] artikel 1, stk. 1, og tredje direktivs[874] artikel 1, stk. 1, samt de tre ovennævnte direktivers beskyttelsesformål, måtte fastslås, at omfattet af begrebet "personskade" var ethvert tab, i det omfang der blev foreskrevet en erstatning herfor i medfør af den forsikredes erstatningsansvar i henhold til de *nationale* bestemmelser, der fandt anvendelse på tvisten, som følge af en krænkelse af personens integritet, hvilket omfattede såvel fysiske som psykiske lidelser.

EU-Domstolen udtalte endvidere i præmis 40, at da de forskellige sprogversioner af andet direktivs artikel 1, stk. 1, i det væsentlige anvender begreberne såvel "legemsskade" som "personskade", må man henholde sig til den almindelige opbygning af og formålet med disse bestemmelser og direktivet. Det bemærkes her ved, at disse begreber supplerer begrebet "materiel skade", og at de nævnte bestemmelser og direktivet navnlig tilsigter at styrke beskyttelse af ofrene. Herefter må der anlægges den brede fortolkning af de nævnte begreber, som er anført i denne doms præmis 38.

EU-Domstolen udtalte ydermere i præmis 41, at det heraf [af det brede skadesbegreb] følger, at immaterielle skader, for hvilke der foreskrives en erstatning i medfør af den forsikredes erstatningsansvar i henhold til de *nationale* bestemmelser, der finder anvendelse på tvisten, er blandt de skader, som der skal betales erstatning for i overensstemmelse med første, andet og tredje direktiv.

EU-Domstolen udtalte endelig i præmis 44, at eftersom skadesbegrebet i første direktivs[875] artikel 1, nr. 2, ikke var yderligere begrænset, var der desuden, i modsætning til hvad den lettiske og litauiske regering havde anført, intet grundlag for at antage, at visse skader, såsom immaterielle skader, i det omfang der skulle betales erstatning herfor i henhold til de *nationale* bestemmelser om erstatningsansvar, som fandt anvendelse, skulle udelukkes fra dette begreb. Af første direktivs artikel 1, nr. 2, fremgår det, at skadelidte er enhver person, der har ret til erstatning for skade forvoldt af et køretøj.

---

[873] Rådets andet direktiv af 30. december 1983 om indbyrdes tilnærmelse af medlemsstaternes lovgivning om ansvarsforsikring for motorkøretøjer (84/5/EØF).
[874] Rådets tredje direktiv af 14. maj 1990 om indbyrdes tilnærmelse af medlemsstaternes lovgivning om ansvarsforsikring for motorkøretøjer (90/232/EØF).
[875] Rådets første direktiv af 24. april 1972 om indbyrdes tilnærmelse af medlemsstaternes lovgivning om ansvarsforsikring for motorkøretøjer og kontrollen med forsikringspligtens overholdelse (72/166/EØF).

Det samme følger af C-22/12, Hassová, afgjort af EU-Domstolen samme dag, 24. oktober 2013. Derudover er samme fortolkning anlagt i sag C-371/12, Petillo, dom af 23. januar 2014, hvor sagsøger blev påkørt, hvilket medførte legemsbeskadigelse.

EU-Domstolen synes ikke at have en konsekvent linje i fortolkningen af begrebet "skade". Af domspraksis kan det således umiddelbart både udledes, at der af pakkerejsedirektivets skadesbegreb kan fortolkes et krav på godtgørelse for ikke-økonomisk skade, og at EU-Domstolen ved nyere praksis alene, ud af de direktiver, der regulerer ansvarsforsikring for motorkøretøjer, fortolker skadesbegrebet til at inkludere et krav om godtgørelse for ikke-økonomisk skade, hvis dette følger af de nationale bestemmelser.

9.6.2.3. EU-lovgivningspraksis om begreberne erstatning og godtgørelse

Begrebet "erstatning" er bl.a. reguleret i artikel 13 i direktiv om håndhævelse af intellektuelle rettigheder[876], der har overskriften erstatning.

Af artikel 13, stk. 1, fremgår det, at medlemsstaterne sikrer, at de kompetente retslige myndigheder på begæring af den forurettede pålægger den krænkende part, der vidste eller med rimelighed burde vide, at hans aktiviteter medførte en sådan krænkelse, at betale rettighedshaveren en erstatning, der står i rimeligt forhold til det tab, denne har lidt som følge af krænkelsen.

Når de retslige myndigheder fastsætter erstatningen,

a) skal de tage hensyn til alle relevante aspekter, såsom negative økonomiske konsekvenser, herunder tabt fortjeneste, som den forurettede har lidt, den krænkende parts uberettigede fortjeneste, og, når det er hensigtsmæssigt, andre elementer end de økonomiske, f.eks. den ikke-økonomiske skade, rettighedshaveren har lidt som følge af krænkelsen

b) eller de kan, som et alternativ til litra a), når det er hensigtsmæssigt, fastsætte erstatningen til et fast beløb på grundlag af elementer, der som minimum svarer til størrelsen af de gebyrer eller afgifter, som den krænkende part skulle have betalt, hvis han havde anmodet om tilladelse til at anvende den pågældende intellektuelle ejendomsrettighed.

Ligebehandlingsdirektivets (direktiv 2006/54/EF) artikel 18 bærer overskriften "erstatning eller godtgørelse". I den engelske sprogversion bærer artikel 18 overskriften "compensation or reparation". Af direktivets artikel 18, 1. pkt., følger det, at medlemsstaterne i deres nationale retsorden indfører de nødvendige bestemmelser for at sikre en reel og effektiv

[876] Europa-Parlamentet og Rådets direktiv af 29. april 2004 om håndhævelsen af intellektuelle ejendomsrettigheder (2004/48/EF).

erstatning eller godtgørelse efter medlemsstatens afgørelse for tab og skader, der er påført en person som følge af en forskelsbehandling på grundlag af køn, således at det har en præventiv virkning og står i et rimeligt forhold til det tab, den pågældende har lidt.

Af ligebehandlingsdirektivets præambelbetragtning nr. 33, fremgår det bl.a., at EU-Domstolen klart har fastslået, at for, at princippet om ligebehandling kan være effektivt, skal den erstatning, der tildeles i tilfælde af overtrædelse, være tilstrækkelig i forhold til det tab, den pågældende har lidt.

9.6.2.4. Persondataloven

Persondatalovens § 69, der er den nationale udmøntning af databeskyttelsesdirektivets artikel 23, fastsætter, at den dataansvarlige, skal erstatte skade, der er forvoldt ved behandling i strid med bestemmelserne i denne lov, medmindre det godtgøres, at skaden ikke kunne have været afværget ved den agtpågivenhed og omhu, der må kræves i forbindelse med behandling af oplysninger.

Selvom det ikke klart følger af bemærkningerne til persondatalovens § 69, er der meget der taler for, at bestemmelsen alene dækker økonomisk skade. Justitsministeriet har bl.a. i de almindelige bemærkninger til lovforslag nr. L 162 af 28. februar 2007 om udvidelse af adgangen til tv-overvågning og styrkelse af retsbeskyttelsen ved behandling af personoplysninger i forbindelse med tv-overvågning anført, at godtgørelse for krænkelse af lovens regler om beskyttelse af den registreredes personlige integritet, der ikke har medført et formuetab, falder uden for persondatalovens § 69. I stedet må et sådant krav i givet fald gøres gældende efter den almindelige regel om godtgørelse i erstatningsansvarslovens § 26.[877]

Det bemærkes dog, at Registerudvalgt i betænkning nr. 1345 anførte, at såvel økonomisk som ikke-økonomisk skade er omfattet af persondatalovens § 69.[878] Det følger dog af bemærkningerne til persondataloven, at bestemmelsen ikke – udover fastsættelse af præsumptionsansvar – indebærer andre ændringer i dansk rets almindelige erstatningsretlige regler.[879] Det må i den forbindelse antages, at der også er tænkt på erstatningsbetingelsen om, at der skal være lidt et *økonomisk* tab.

[877] Se bl.a. punkt 7.6.2. i Justitsministeriets lovforslag nr. 162 af 28. februar 2007, FT 2006/07 om udvidelse af adgangen til tv-overvågning og styrkelse af retsbeskyttelsen ved behandling af personoplysninger i forbindelse med tv-overvågning.
[878] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 521.
[879] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 69.

Økonomisk tab som følge af overtrædelser af persondataloven vil bl.a. kunne forekomme ved ukorrekt persondatabehandling i forbindelse med kreditoplysning, e-handel og i ansættelsessituationer. Erstatningskrav efter persondatalovens § 69 skal indbringes for domstolene og vil ikke kunne forelægges tilsynsmyndighederne.

Der findes ikke trykt retspraksis, hvor domstolene har tilkendt erstatning efter persondatalovens § 69. Der er dog retspraksis – i form af U 2005.1639 V gengivet nedenfor – hvor domstolene har taget stilling til spørgsmålet om erstatning efter persondatalovens § 69 uden at finde et grundlag herfor.

Registerudvalget anførte i betænkning nr. 1345, at direktivets artikel 23 må antages at skulle forstås således, at det påhviler medlemsstaterne at fastsætte et præsumptionsansvar for den dataansvarliges uretmæssige behandling af oplysninger om registrerede personer.[880]

Registerudvalget anførte endvidere i betænkning nr. 1345, at direktivets artikel 23 herudover ikke nødvendiggør, at der i lovgivningen fastsættes særlige regler vedrørende dataansvarliges erstatningsansvar. Udvalget anbefalede derfor, at dansk rets almindelige erstatningsregler, herunder reglerne om kausalitet, adækvans, egen skyld mv., fortsat skulle finde anvendelse ved bedømmelse af, om den dataansvarlige var erstatningsansvarlig over for den registrerede.[881]

Det følger af persondataloven med kommentarer, at det er den registrerede (skadelidte), der har bevisbyrden for, at der er årsagssammenhæng mellem den lovstridige behandling og tabet, samt at det økonomiske tab er en påregnelig følge af den lovstridige behandling samt for, at der rent faktisk er lidt et tab. Derimod er det den dataansvarlige, der skal bevise, at der ikke er handlet culpøst.[882]

Derudover følger det af persondataloven med kommentarer, at godtgørelse for tort i anledning af en krænkelse af lovens regler om beskyttelse af den registreredes personlige integritet, der ikke medfører formuetab, alene kan kræves i det omfang, at lovgivningen i øvrigt giver adgang hertil. Det vil i praksis sige i medfør af erstatningsansvarslovens § 26, hvorefter det af stk. 1 fremgår, at den, der er ansvarlig for en retsstridig krænkelse af en andens frihed, fred, ære eller person, skal betale den forurettede godtgørelse for tort.[883]

[880] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 388.
[881] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 388.
[882] Persondataloven med kommentarer (2015), s. 654f.
[883] Persondataloven med kommentarer (2015), s. 655.

9.6.2.5. Dansk erstatningsret

Det følger endelig af dansk rets almindelige erstatningsretlige regler, som er fastsat af retspraksis, at hvis der er flere erstatningsansvarlige for den samme skade, er det hovedreglen, at de hæfter solidarisk over for skadelidte, hvilket er ensbetydende med, at skadelidte kan kræve hele erstatningsbeløbet hos hvem af skadevolderne, skadelidte ønsker, og således at skadevolderne (alle) er frigjort over for skadelidte, når skadelidte har modtaget erstatningsbeløbet.

Som eksempel på retspraksis om solidarisk hæftelse, kan henvises til en sag ved Østre Landsret, U 1979.927 Ø, hvor A, B og C alle, som medvirkende til et overfald på N, blev pålagt solidarisk medansvar for legemsskade. For C's vedkommende blev det i straffedommen lagt til grund, at han vel havde kastet en flaske i panden på N, men at der ikke herved var blevet tilføjet N skade på legeme eller helbred. Under en efterfølgende erstatningssag fandtes C imidlertid ved sin tilstedekomst sammen med de to andre og ved sit kast med flasken at have medvirket til forholdet på en sådan måde, at der måtte påhvile ham solidarisk medansvar for den legemsskade, N pådrog sig.

Det følger af erstatningsansvarslovens § 25, stk. 1, at den indbyrdes fordeling af erstatningsbyrden mellem flere solidarisk erstatningsansvarlige foretages efter, hvad der under hensyn til ansvarets beskaffenhed og omstændighederne i øvrigt må anses for rimeligt.

Det er således den almindelige regel i dansk erstatningsret, at i den situation, at en erstatningsansvarlig har måtte betale et erstatningsbeløb, der er større end ansvarsfordelingen mellem de erstatningsansvarlige, så har denne erstatningsansvarlige som regel adgang til at søge regres hos de andre erstatningsansvarlige.

Der skelnes traditionelt i dansk erstatningsret mellem integritetskrænkelser (også benævnt materiel skade) og ikke-integritetskrænkelser (også benævnt immateriel skade), jf. A. Vinding Kruse, Erstatningsretten, 5. udgave, 1989, s. 85. Ved integritetskrænkelser forstås skader forvoldt med fysiske midler på det menneskelige legeme eller på ting, dyr eller fast ejendom.[884] Alle andre skader henføres til området for ikke-integritetskrænkelser. Sondringen går altså på, om skaden er fysisk eller ikke-fysisk forvoldt. Ikke-integritetskrænkelser omfatter således både krænkelser af forfatter- og kunstnerrettigheder, patenter, varemærker mv., retsstridig adfærd under erhvervsudøvelse, såsom utilbørlig markedsføring i øvrigt (økonomisk skade) samt krænkelser af privatlivets fred, æreskrænkelser, navnekrænkelser osv. (ikke-økonomisk skade). Der er en række fællestræk ved ikke-integritetskrænkelser, som i større eller mindre grad går igen hos de fleste af dem. Krænkelserne vil oftere resul-

[884] A. Vinding Kruse, Erstatningsretten, 5. udgave, 1989, s. 85.

tere i ikke-økonomiske skader end ved integritetskrænkelser. Hvis der derimod foreligger en økonomisk skade, vil denne ofte være betydeligt vanskeligere at dokumentere størrelsen af, end hvor det drejer sig om integritetskrænkelser.[885]

Det fremgår derudover, at sondringen mellem integritetskrænkelser og ikke-integritetskrænkelser (almindelig formueskade) er tillagt afgørende betydning ved spørgsmålet om, hvilke goder der bør tillægges erstatningsretlig eller anden retlig beskyttelse. På en række områder, herunder f.eks. ophavs- og konkurrenceretten, vil det traditionelle erstatningskrav ofte være af mindre interesse, fordi det som regel er meget vanskeligt at føre bevis for, at krænkelsen har medført et tab af en bestemt størrelse.[886] For disse retsområders vedkommende følger det af artikel 13 i direktivet om håndhævelse af intellektuelle rettigheder, der er gengivet ovenfor, og som den danske lovgivning på dette område er udformet på baggrund af, hvordan erstatningen fastsættes. Endelig vil det for adskillige ikke-integritetskrænkelsers vedkommende være et langt større behov for regler om godtgørelse for ikke-økonomisk skade, hvilket især gælder ved krænkelser af en persons frihed, ære og fred.[887] På baggrund heraf kan det udledes, at når vi i en dansk kontekst bruger ordet erstatning og immateriel skade i samme sætning, så handler det om et økonomisk tab, hvilket kan være et omsætningstab.

Andre steder i den erstatningsretlige litteratur inddeles skadesbegrebet ligeledes for det første i person- og tingsskade samt skader, der opstår som følge af en person- og tingsskade (integritetskrænkelser), og for det andet i skader, som indtræder uden sammenhæng med, at nogen lider person- og tingsskade, såkaldt almindelig (eller "ren") formueskade (ikke-integritetskrænkelser).[888]

Der skelnes i dansk erstatningsret mellem erstatning for økonomisk skade og erstatning for ikke-økonomisk skade – normalt kaldet "godtgørelse". Dansk erstatningsret bygger på det princip, at der som hovedregel kun kan kræves erstatning for økonomisk skade. Udgangspunktet er, at den skadelidte økonomisk skal stilles, som om skaden ikke var sket. Godtgørelse for ikke-økonomisk skade gives derimod alene i særlige tilfælde, hvor der findes at være et særligt behov herfor. Tilkendelse af godtgørelse for ikke-økonomisk skade forudsætter, at der er en særlig hjemmel i lovgivningen hertil.[889]

Sådan særlig hjemmel findes i erstatningsansvarsloven, hvor det af § 1, stk. 1, følger, at den, der er erstatningsansvarlig for personskade, skal betale erstatning for tabt arbejdsfor-

[885] A. Vinding Kruse, Erstatningsretten, 5. udgave, 1989, s. 76.
[886] A. Vinding Kruse, Erstatningsretten, 5. udgave, 1989, s. 305f.
[887] A. Vinding Kruse, Erstatningsretten, 5. udgave, 1989, s. 306.
[888] Bo Von Eyben m.fl., Lærebog i erstatningsret, 8. udgave, 2015, s. 30f.
[889] Betænkning 1412/2002 om godtgørelse til efterladte ved dødsfald, s. 12.

tjeneste, helbredsudgifter og andet tab som følge af skaden, samt en godtgørelse for svie og smerte.

Erstatningsansvarsloven regulerer derefter i §§ 2 og 5-7 i hvilket omfang og med hvilket beløb den erstatningsansvarlige skal betale erstatning for henholdsvis tabt arbejdsfortjeneste og for erhvervsevnetab. Endelig regulerer erstatningsansvarslovens §§ 3-4, betingelserne for i hvilket omfang og med hvilket beløb, den erstatningsansvarlige skal betale skadelidte en godtgørelse. Af erstatningsansvarslovens § 3 fremgår det således, at den, der er erstatningsansvarlig for personskade efter lovens § 1, efter faste takster, skal yde skadelidte godtgørelse for dennes ikke-økonomiske skade i form af svie og smerte pr. dag, hvor skadelidte er syg.

Godtgørelsesregler, der er udtryk for en kompensation for en særlig krænkelse af en person, er f.eks. erstatningsansvarslovens § 26 om godtgørelse for tort mv. samt de forskellige specialregler om godtgørelse for tort, f.eks. ophavsretslovens § 83, retsplejelovens § 639 (ulovlig arrest) og retsplejelovens §§ 1018 a-d (erstatning i anledning af strafferetlig forfølgning). Tort er navnlig en krænkelse af en persons selv- og æresfølelse, dvs. opfattelsen af eget værd og omdømme.[890]

Af ophavsretslovens § 83 følger det af stk. 1, at den, som forsætligt eller uagtsomt overtræder en af de i §§ 76 og 77 nævnte bestemmelser, skal betale forurettede *et rimeligt vederlag* for udnyttelsen. Af stk. 2, følger det, at den samme også skal betale en *erstatning* for den yderligere skade, som overtrædelser har medført. Endelig følger det af stk. 3, at i sager som nævnt i stk. 1, kan der derudover fastsættes en *godtgørelse* til den forurettede for ikke-økonomisk skade.

En lignende bestemmelse kan bl.a. findes i patentlovens § 58. I begge love er der en klar sondring mellem, hvornår der skal betales en erstatning, og hvornår der fastsættes en godtgørelse.

Som et eksempel fra international ret kan nævnes artikel 41 i Den Europæiske Menneskerettighedskonvention (EMRK), hvorefter Menneskerettighedsdomstolen skal tilkende den forurettede part en passende erstatning, hvis den pågældende stat kun tillader delvis skadesløsholdelse.[891] I praksis udmåler EMD bl.a. kompensation for økonomisk skade (pecu-

[890] Betænkning 1412/2002 om godtgørelse til efterladte ved dødsfald, s. 13.
[891] Betænkning 1412/2002 om godtgørelse til efterladte ved dødsfald, s. 13.

niary damage) og ikke-økonomisk skade (non-pecuniary damage).[892] EMRK er inkorporeret i dansk ret ved lov om den europæiske menneskerettighedskonvention.

I nogle tilfælde synes præventive hensyn at være tillagt betydeligt vægt, dvs. at godtgørelsesreglerne tilsigter at bidrage til, at bestemte retsstridige forhold undgås. Som eksempel herpå kan nævnes reglerne i ligebehandlingslovens §§ 14-16 om godtgørelse bl.a. ved manglende ligebehandling af mænd og kvinder med hensyn til ansættelse, forflyttelse, forfremmelse og uddannelse samt ved afskedigelse i strid med ligebehandlingsloven. Det antages, at dansk rets almindelige erstatningsregler gælder ved siden af disse særlige godtgørelsesregler. Ligebehandlingsloven gennemfører EU-direktivet om ligebehandling, der bl.a. indeholder regler om erstatning eller godtgørelse som følge af forskelsbehandling. EU-Domstolen har herom udtalt, at medlemsstaternes regler skal sikre erstatningens effektivitet og afskrækkende virkning.[893]

Ligebehandlingslovens § 14-16 henhører under lovens kapitel 6 om godtgørelse, bevisbedømmelse mv. Bestemmelserne vedrører alene godtgørelse og behandler således ikke spørgsmålet om erstatning. Det følger af bemærkningerne til ligebehandlingslovens § 14, at der ikke er noget til hinder for, at der ved siden af godtgørelsen eller alene ydes erstatning efter de almindelige erstatningsretlige regler, f.eks. når den pågældende har lidt et egentligt økonomisk tab.

Såfremt der ikke er en anden særlig hjemmel til tilkendelse af godtgørelse for ikke-økonomisk skade, kan der efter erstatningsansvarslovens § 26 i visse tilfælde tilkendes godtgørelse for tort. Det følger af erstatningsansvarslovens § 26, stk. 1, at den, der er ansvarlig for en retsstridig krænkelse af en andens frihed, fred, ære eller person, skal betale den forurettede godtgørelse for tort.

Tortgodtgørelse efter erstatningsansvarslovens § 26 kræver opfyldelse af en række andre betingelser, der ikke følger af persondataloven, herunder, at krænkelsen skal være grov, og at det i almindelighed er forudsat, at den retsstridige handling på objektivt grundlag skal være egnet til at integritetskrænke. Dog er det her – i modsætning til de almindelige betingelser for tilkendelse af erstatning – ikke påkrævet at føre bevis for et økonomisk tab.

9.6.2.6. Dansk retspraksis

Sø- og Handelsretten tilkendte i dom U 2007.1603 S en erstatning for tab i form af mistet omsætning, der blev fastsat skønsmæssigt til 250.000 kr. I sagen blev Sikkerhedsstyrelsen

[892] Peer Lorenzen m.fl., Den Europæiske Menneskerettighedskonvention med kommentarer, art. 10 – 59 samt Tillægsprotokollerne, 3. udgave, 2011, s. 1159.
[893] Betænkning 1412/2002 om godtgørelse til efterladte ved dødsfald, s. 14.

gjort erstatningsansvarlig overfor Jysk A/S' og Eng Danmark A/S' på grundlag af en række sagsbehandlingsfejl og ved manglende rettelse af oplysninger på sin og Forbrugerstyrelsens hjemmeside. Sikkerhedsstyrelsen fandtes herved at have pådraget sig et erstatningsansvar for tab i form af mistet omsætning og merarbejde, men ikke goodwill, tort eller øvrige tabsposter. Det fremgår ikke direkte af dommen, men det må antages, at erstatningspligt og –sum følger af almindelige retsgrundsætninger. Der var i sagen tale om en immateriel økonomisk skade, i og med, at det, som sagsøgerne i tilstrækkelig grad kunne dokumentere og fik tilkendt en erstatning for, var tab i form af mistet omsætning.

Østre Landsret tilkendte i dom U 2001.510 Ø den erstatningssøgende E en erstatning på 10.000 kr. på grundlag af en overtrædelse af EMRK artikel 6, stk. 1. Erstatningen blev fastsat i medfør af retsplejelovens § 1018 h. E var den 6. maj 1994 impliceret i et færdselsuheld. Ved byretsdom af 14. juni 1995 blev E idømt bøde og frakendt førerretten betinget. Ved landsrettens dom af 12. marts 1998 blev E frifundet for påstanden om betinget frakendelse. E fremsatte den 23. marts 1998 krav om erstatning, og kravet blev den 26. april 2000 indbragt for retten. Byretten anførte, at tidsforløbet udgjorde en krænkelse af EMRK artikel 6, stk. 1, henset bl.a. til, at det drejede sig om en ukompliceret færdselssag.

Højesteret tog i U 2017.98 H stilling til, om der skulle udbetales tortgodtgørelse til to ansatte i en situation, hvor der mellem parterne var enighed om, at Banedanmarks praksis med at indscanne, opbevare og bruge lægeerklæringer i personalemapper indebar en overtrædelse af persondatalovens § 7, stk. 1. Højesteret konkluderede, at Banedanmarks praksis ikke indebar en sådan retsstridig krænkelse af de berørte, at der var grundlag for tortgodtgørelse i medfør af erstatningsansvarslovens § 26, stk. 1. Der blev i den forbindelse lagt vægt på, at de pågældende oplysninger befandt sig på et »lukket« journalsystem for personalesager, hvortil kun en begrænset kreds af personer, der i øvrigt beskæftigede sig med personalesager i Banedanmark, havde haft adgang. Det blev i forbindelse med spørgsmålet om tortgodtgørelse desuden lagt til grund, at Banedanmarks håndtering af oplysningerne ikke havde påvirket den materielle rigtighed af de tre personalesagers udfald.

Vestre Landsret tog i U 2005.1639 V stilling til en arbejdsgivers, B's, læsning af en ansats, A's, private e-mailkorrespondance, hvilket medførte en uberettiget ophævelse af ansættelsesforholdet for A. Det blev i sagen lagt til grund, at B ved en tilfældighed blev bekendt med e-mailkorrespondancen, og at det ikke uden at læse korrespondancen var muligt at konstatere, at den var privat. Der forelå derfor ikke en krænkelse fra B's side, som kunne danne grundlag for godtgørelse efter erstatningsansvarslovens § 26. Da A ikke havde lidt noget økonomisk tab ved, at B var blevet bekendt med korrespondancen, var der heller ikke grundlag for erstatning i medfør af persondatalovens § 69.

Østre Landsret tog i dom U 2004.273 Ø stilling til et detektivbureaus (D) overvågning – på arbejdsgiverens (B) anmodning – af en sygemeldt medarbejder (A) for at klarlægge, om sygemeldingen var reel. B havde fremsendt en række oplysninger om A til D, som, ifølge landsretten, gik videre end hvad persondataloven hjemlede. Dette fandtes dog ikke at indebære en sådan krænkelse af medarbejderen, at der var grundlag for tortgodtgørelse i medfør af erstatningsansvarslovens § 26.

Sø- og handelsretten tog i dom U 2008.727/2S stilling til om en arbejdsgivers tv-overvågning af en ansat berettigede til tortgodtgørelse efter erstatningsansvarslovens § 26. Den butiksansatte CL blev tv-overvåget af sin arbejdsgiver fra dennes private bopæl i en halv time til tre kvarter. Overvågningen var ikke arbejdsmæssigt eller sikkerhedsmæssigt begrundet. Overvågningen medførte, at der blev indsamlet oplysninger (billeder) af CL til et andet formål, end hvad der må antages at have været hende bekendt, og overvågningen var således i strid med persondatalovens § 5, stk. 1 og 2, om god databehandlingsskik, og om at indsamling af oplysninger skulle ske til udtrykkeligt angivne og saglige formål. Endvidere var etableringen af overvågning i strid med en aftale om kontrolforanstaltninger indgået mellem LO og DA. Der forelå således en retsstridig handling, der berettigede CL til tortgodtgørelse efter erstatningsansvarslovens § 26. Det forhold, at Arbejdsretten havde pålagt arbejdsgiveren bod for overtrædelse af aftalen mellem LO og DA om kontrolforanstaltninger, kunne ikke føre til frifindelse. Efter overvågningens karakter og udstrækning blev tortgodtgørelsen fastsat til 25.000 kr.

Vestre Landsret tog i dom U 2000.2334 V – uden at referere direkte til persondataloven, stilling til en politistations videregivelse til en tv-station af en optagelse af to personer (A og B), der blev filmet af et overvågningskamera i en forretning, der forinden var blevet udsat for tyveri. Af tv-stationens udsendelse fremgik det, at A og B var mistænkt, og at politiet ønskede oplysninger til identifikationen af dem. A og B blev anholdt og sigtet for tyveriet, men påtale blev opgivet. Landsretten fastsatte godtgørelse til i alt 15.000 kr. til hver i medfør af erstatningsansvarslovens § 26, jf. retsplejelovens § 1018 h.

Højesteret fastsatte i dom U 2011.2343 H, at en kommunes (H) videregivelse af oplysninger om en mistanke om et alkoholmisbrug som led i en potentiel arbejdsgivers (S) indhentelse af referenceoplysninger, var en retsstridig videregivelse i medfør af persondatalovens § 7, stk. 1. Højesteret fandt det ikke godtgjort, at A ville have opnået ansættelse hos S, hvis oplysningerne ikke var blevet videregivet, hvorfor A ikke fandtes at have krav på erstatning som medfør af den retsstridige videregivelse. A fik dog i medfør af erstatningsansvarslovens § 26 tilkendt 25.000 kr. i tortgodtgørelse fra H.

9.6.3. Databeskyttelsesforordningen

Det fremgår af begrundelsen til forslaget til databeskyttelsesforordningen, at forordningens artikel 82 (som var en del af artikel 77 i forslaget) udvider retten til erstatning for den forvoldte skade fra dataansvarlige og databehandlere og præciserer ansvaret for solidarisk hæftelse og regression.[894]

Det følger af forordningens præambelbetragtning nr. 147, at når forordningen indeholder specifikke kompetenceregler, navnlig for så vidt angår sager om adgang til retsmidler, herunder erstatning, mod en dataansvarlig eller databehandler, bør de almindelige kompetenceregler i Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012 ikke berøre anvendelsen af sådanne specifikke regler.

9.6.3.1. Databeskyttelsesforordningens artikel 82, stk. 1

Det følger af forordningens artikel 82, stk. 1, at enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren.

Forordningens artikel 82, stk. 1, ses i vidt omfang at videreføre retten til erstatning i direktivets artikel 23.

Det følger bl.a. af præambelbetragtning nr. 146, at begrebet "skade" bør fortolkes bredt i lyset af retspraksis ved Domstolen, således at det fuldt ud afspejler formålene for denne forordning. Det fremgår endvidere af betragtningen, at dette ikke berører eventuelle erstatningskrav for skade som følge af overtrædelse af andre bestemmelser i EU-retten eller medlemsstaternes nationale ret, at behandling, der overtræder denne forordning, også omfatter behandling, der overtræder delegerede retsakter og gennemførelsesretsakter vedtaget i henhold til denne forordning og til medlemsstaternes nationale ret, der præciserer bestemmelserne i denne forordning, og at registrerede bør have fuld erstatning for den skade, som de har lidt.

Det fremgår nu eksplicit i forordningen, at der skal gælde et erstatningsansvar for *materiel* eller *immateriel* skade, hvor direktivet alene nævner *skade*. Materiel skade er, som nævnt ovenfor, allerede omfattet af persondatalovens § 69, hvis et økonomisk tab kan konstateres. Derudover må immateriel skade også anses for at være omfattet af persondatalovens § 69, i de tilfælde, hvor et økonomisk tab kan konstateres, hvilket efter omstændighederne kan være et tab i form af mistet omsætning, jf. U 2007.1603S, refereret ovenfor. Dette kunne eksempelvis være tilfældet ved en uberettiget offentliggørelse af personoplysninger, som er

[894] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), s. 16.

en immateriel skade, der kan medføre erstatning, hvis der kan dokumenteres at være lidt et økonomisk tab, herunder et omsætningstab.

Det følger ikke nærmere af ordlyden af artikel 82, stk. 1, hvad der må forstås ved begreberne materiel eller immateriel skade. Det følger dog, at begrebet "skade", i lyset af retspraksis ved EU-Domstolen, skal fortolkes bredt, således at det afspejler formålene i forordningen. På området for pakkerejser har EU-Domstolen fortolket begrebet "skade" til også at omfatte godtgørelse for ikke-økonomisk skade. EU-Domstolen har dog i nyere praksis ved udmåling af erstatning i forbindelse med trafikuheld fortolket dette til alene at gælde i det omfang, der blev foreskrevet en erstatning herfor i medfør af den forsikredes erstatningsansvar i henhold til de nationale bestemmelser, der fandt anvendelse på tvisten, jf. den refererede retspraksis fra EU-Domstolen. Det fremstår ikke klart, hvad der må forstås ved en bred fortolkning af begrebet "skade" i EU-Domstolens praksis, jf. præambelbetragtning nr. 146, herunder om der efter artikel 82, stk. 1, skal kunne tilkendes en "erstatning" for ikke-økonomisk skade, såfremt der i national ret er foreskrevet en erstatning herfor.

EU-lovgiver er heller ikke konsekvent i anvendelsen af henholdsvis begreberne "erstatning" og "godtgørelse", ligesom der heller ikke kan konstateres konsistens i brugen af begreberne "materiel/immateriel skade" og "økonomisk/ikke-økonomisk skade". Dette ses bl.a. afspejlet i de to direktiver, der er gengivet ovenfor. I ligebehandlingsdirektivet ses der at være en klar sondring mellem erstatning på den ene side og godtgørelse på den anden. I direktivet om intellektuel ejendomsret følger det derimod, at et af de aspekter, der skal tages hensyn til under udmåling af *erstatning*, hvis det er hensigtsmæssigt, er andre elementer end de økonomiske, f.eks. den ikke-økonomiske skade, rettighedshaveren har lidt som følge af krænkelsen.

Databeskyttelsesforordningens formål følger af artikel 1, stk. 2 og 3. Af artikel 1, stk. 2, følger det, at forordningen beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger. Af artikel 1, stk. 3, følger det, 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.

Forordningens artikel 82, stk. 1, var i artikel 77, stk. 1, i Kommissionens oprindelige forslag, affattet på følgende måde: "Enhver, som har lidt skade som følge af en ulovlig behandling eller enhver anden handling, der er uforenelig med denne forordning, har ret til

erstatning for den forvoldte skade fra den [dataansvarlige] eller [databehandleren]".[895] Derudover var præambelbetragtning nr. 118, 1. pkt., (den nuværende betragtning nr. 146) affattet således: "Personer, der lider skade som følge af en ulovlig behandling, bør have ret til erstatning fra den [dataansvarlige] eller [databehandleren]".[896]

Artikel 29-gruppen har om det oprindelige forordningsforslags artikel 77 bl.a. udtalt, at arbejdsgruppen finder det nødvendigt at afklare (i en betragtning), at ordet "skade" ikke kun henviser til materiel skade, men også omfatter andre former for skade (immateriel skade).[897]

I Europa-Parlamentets betænkning af 21. november 2013 fra udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender blev der foreslået ændringer til forordningsforslagets præambelbetragtning nr. 118 og artikel 77, stk. 1. Til betragtning nr. 118 ønskedes der indsat personer, der lider skade, *uanset om den er økonomisk eller ej*. Til artikel 77, stk. 1, ønskedes der indsat "enhver, som har lidt skade, *herunder ikke-økonomisk skade*…"[898]

Af Rådets generelle indstilling af 11. juni 2015 nævnes det i indledningen, at Rådet har ønsket at modificere bl.a. præambelbetragtning nr. 118 og artikel 77.[899] Præambelbetragtning nr. 118, der i al væsentlighed kan genfindes i den endelige forordnings præambelbetragtning nr. 146, blev af Rådet affattet på ny og lyder således: "Personer, der lider skade som følge af en behandling, der ikke er i overensstemmelse med denne forordning, bør have ret til erstatning fra den dataansvarlige eller databehandleren. Denne bør fritages for erstatningsansvar, hvis det bevises, at den pågældende ikke på nogen måde er skyld i den forvoldte skade (…) Begrebet "skade" skal fortolkes bredt i lyset af retspraksis ved den Europæiske Unions Domstol, således at det fuldt ud afspejler målene for denne forordning".[900] Artikel 77, stk. 1, der i al væsentlighed kan genfindes i den nuværende artikel 82, stk. 1, blev også affattet på ny og lyder således: "Enhver, som har lidt materiel eller immateriel skade som følge af en behandling, der ikke er i overensstemmelse med denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren."

Det må af det oplistede hændelsesforløb kunne udledes, at Rådet ikke ønskede, at der skulle henvises til ikke-økonomisk skade, hvilket EU-lovgiver som sådan endte med at følge.

---

[895] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), s. 94.
[896] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), s. 37.
[897] Opinion 01/2012 on the data protection reform proposals: WP 191, s. 24, fra den 23. marts 2012.
[898] Europaparlamentets betænkning fra udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender af 21. november 2013 (A7-0402/2013).
[899] Rådets generelle indstilling af den 11. juni 2015 (9565/15), s. 2.
[900] Rådets generelle indstilling af den 11. juni 2015 (9565/15), s. 63.

Forordningens artikel 82 bærer overskriften ”ret til erstatning og erstatningsansvar”. I den engelske version bærer artikel 82 overskriften ”right to compensation and liability”, ligesom det også var tilfældet i ligebehandlingsdirektivets artikel 18, hvor ”erstatning” i den engelske sprogversion er ”compensation”. Derudover fastsætter forordningen ikke i artikel 82, stk. 1, de nærmere betingelser for at fastslå erstatningsansvaret og den deraf følgende erstatningssum, i modsætning til området for administrative bøder, jf. forordningens artikel 83, stk. 1-6, hvor forordningen er meget udtrykkelig i forhold til bødestørrelserne.

Endelig sondres der efter dansk erstatningsret overordnet set mellem integritetskrænkelser (materiel skade) og ikke-integritetskrænkelser (immateriel skade). Derefter sondres der for begge skadestyper mellem økonomisk og ikke-økonomisk skade, da der som udgangspunkt, efter dansk ret, alene kan opnås erstatning for *økonomisk* skade (der dog godt kan være immateriel, f.eks. et omsætningstab), jf. gengivelsen af gældende ret ovenfor. Dette taler imod, at der alene ud fra forskellen mellem direktivets artikel 23 om ”skade” og forordningens artikel 82, stk. 1, om ”materiel eller immateriel skade” kan udledes, at det med forordningen er tiltænkt, at der også skal gives erstatning for ikke-økonomisk skade efter artikel 82, i hvert fald ikke i situationer, hvor der nationalt ikke er tradition for at give erstatning for ikke-økonomiske tab.

På det foreliggende grundlag, herunder med den foreliggende praksis fra EU-Domstolen og EU-lovgiver, er der således ikke tilstrækkeligt grundlag for at fastslå, at *godtgørelse* for ikke-økonomisk skade er omfattet af retten til *erstatning* for materiel eller immateriel skade efter artikel 82, stk. 1. I hvert fald ikke, hvis der i en medlemsstat ikke normalt uden særskilt hjemmel er mulighed for erstatning for ikke-økonomisk tab. Immateriel skade i forordningens forstand må, i en dansk kontekst, antageligvis forstås som den almindelige eller rene formueskade, som er lidt som følge af overtrædelse af forordningens bestemmelser, hvilket f.eks. kan være et tab i form af mistet omsætning eller fralæggelse af den retsstridigt indvundne berigelse.

Derudover fremgår det i øvrigt bl.a. af forordningens præambelbetragtning nr. 75, at risiciene for fysiske personers rettigheder og frihedsrettigheder, af varierende sandsynlighed og alvor, kan opstå som følge af behandling af personoplysninger, der kan føre til fysisk, materiel eller immateriel skade, navnlig hvis behandlingen kan give anledning til forskelsbehandling, identitetstyveri eller –svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser, hvilke eksempler i øvrigt også peger i retningen af, at der med artikel 82 alene er tiltænkt erstatning for økonomisk skade.

Forordningens artikel 82, stk. 1, ændrer ikke på den mulighed, der eksisterer efter dansk ret, til i visse tilfælde, at udbetale godtgørelse for tort i medfør af erstatningsansvarslovens § 26 for en ikke-økonomisk skade. En sådan bestemmelse må anses for at være en sanktion efter forordningens artikel 84, der er med til at sikre forordningens effektive efterlevelse. For nærmere om forordningens artikel 84 henvises til afsnit 9.11. om sanktioner.

Artikel 82, stk. 1, udvider gældende ret ved at også databehandlere kan være erstatningsansvarlige.

9.6.3.2. Databeskyttelsesforordningens artikel 82, stk. 2

Det følger af forordningens artikel 82, stk. 2, 1. pkt., at enhver dataansvarlig, der er involveret i behandling, hæfter for den skade, der er forvoldt af behandling, der overtræder denne forordning.

Bestemmelsen er i vidt omfang en videreførelse af ordlyden af direktivets artikel 23, og persondatalovens § 69. Dog forudsættes det i bestemmelsen med ordet *enhver*, at der kan forekomme situationer, hvor flere dataansvarlige er involveret i behandling, og som dermed også kan være erstatningsansvarlige.

Af forordningens artikel 82, stk. 2, 2. pkt., følger det, at en databehandler kun hæfter for den skade, der er forvoldt af behandling, hvis pågældende ikke har opfyldt forpligtelser i denne forordning, der er rettet specifikt mod databehandlere, eller hvis pågældende har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser.

Det følger af direktivets artikel 23 og af persondatalovens § 69, at det alene er for den dataansvarlige, at der heri kan findes et ansvarsgrundlag. Det bemærkes dog, at en databehandler kan være erstatningsansvarlig efter en culpanorm. Det er dermed nyt i forhold til gældende ret, at ansvarsgrundlaget for en databehandler under nærmere fastlagte omstændigheder – navnlig hvis databehandleren ikke overholder de forpligtelser, som følger af forordningen - er reguleret af forordningens artikel 82, stk. 2. Dette kan f.eks. være tilfældet, hvis databehandleren uden godkendelse fra den dataansvarlige gør brug af en anden databehandler, jf. forordningens artikel 28, stk. 2.

9.6.3.3. Databeskyttelsesforordningens artikel 82, stk. 3

Det følger af forordningens artikel 82, stk. 3, at en dataansvarlig eller databehandler er fritaget for erstatningsansvar i henhold til stk. 2, hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden.

Af præambelbetragtning nr. 146, præciseres det bl.a., at det er den dataansvarlige eller databehandleren der må bevise, at den pågældende ikke er ansvarlig for den forvoldte skade.

Persondatalovens § 69 præciserer hvilke momenter, der er relevante for en vurdering af, om den dataansvarlige har handlet culpøst. I persondataloven forudsættes det, at vurderingen af, om den dataansvarlige har handlet erstatningspådragende skal ske på baggrund af en kutyme betragtning om, hvad der almindeligvis må kræves af en dataansvarlig.

Det fastsættes ikke i forordningens artikel 82, hvilke momenter der er væsentlige i vurderingen af, om den dataansvarlige eller databehandleren har et ansvar for den skade, som den registrerede er blevet påført. Af den grund må det antages, at en vurdering af skyldsspørgsmålet, der fastsættes på baggrund af en kutyme betragtning, ikke er i uoverensstemmelse med forordningens artikel 82, og vil kunne opretholdes.

Det i bestemmelsen fastsatte præsumptionsansvar, følger allerede af direktivets artikel 23, stk. 2, hvorfor der er tale om en videreførelse af gældende ret.

9.6.3.4. Databeskyttelsesforordningens artikel 82, stk. 4 og 5

Det følger af forordningens artikel 82, stk. 4, at hvis mere end én dataansvarlig eller databehandler eller både en dataansvarlig og en databehandler er involveret i den samme behandling, og hvis de i henhold til stk. 2 og 3 er ansvarlige for skader, der er forvoldt af behandling, hæfter de solidarisk for hele skaden for at sikre fuld erstatning til den registrerede.

Derudover følger det af forordningens artikel 82, stk. 5, at hvis en dataansvarlig eller en databehandler i overensstemmelse med stk. 4 har betalt fuld erstatning for den forvoldte skade, har den pågældende dataansvarlige eller databehandler ret til at kræve den del af erstatningen, der svarer til andres del af ansvaret for skaden, tilbage fra de andre dataansvarlige eller databehandlere, der er involveret i den samme behandling, i overensstemmelse med betingelserne i stk. 2.

Det fremgår bl.a. af præambelbetragtning nr. 146, at hvis dataansvarlige eller databehandlere er inddraget i den samme retssag i overensstemmelse med medlemsstaternes nationale ret, kan erstatning fordeles i henhold til den enkelte dataansvarliges eller databehandlers ansvar for den skade, der er forvoldt af behandlingen, forudsat at der sikres fuld erstatning til den registrerede, som har lidt skaden.

Det fremgår hverken af ordlyden af direktivets artikel 23, eller af ordlyden af persondatalovens § 69, om der i en situation, hvor flere dataansvarlige hæfter solidarisk, gælder en ret

for en dataansvarlig til at søge regres i det tilfælde, at denne har betalt fuld erstatning for den forvoldte skade, hvor andre dataansvarlige har et medansvar.

Det følger dog om erstatningsansvaret i persondatalovens § 69, at det er dansk rets almindelige erstatningsbetingelser, der finder anvendelse, hvorefter det er udgangspunktet, at såfremt der er flere erstatningsansvarlige, hæfter de solidarisk med mulighed for efterfølgende regres.

Forordningen artikel 82, stk. 4 og 5, suppleres af erstatningsansvarslovens § 25, hvor det af stk. 1 fremgår, at den indbyrdes fordeling af erstatningsbyrden mellem flere solidarisk erstatningsansvarlige foretages efter, hvad der under hensyn til ansvarets beskaffenhed og omstændighederne i øvrigt må anses for rimeligt. Af § 25, stk. 2, følger det bl.a., at såfremt en eller flere af de erstatningsansvarlige er dækket af en ansvarsforsikring, kan der – i visse tilfælde – ved den indbyrdes fordeling af erstatningsbyrden mellem skadevolderne tages hensyn til foreliggende ansvarsforsikringer.

Derudover suppleres artikel 82, stk. 5, også af erstatningsansvarslovens § 27, stk. 2, hvoraf det følger, at aftaler om fravigelse af en række bestemmelser (herunder § 25) før en skades indtræden, er ugyldige, såfremt fravigelsen er til ugunst for den erstatningsansvarlige. En lignende bestemmelse for så vidt angår fravigelser til ugunst for den erstatningsberettigede følger af stk. 1.

Det følger dog af § 27, stk. 2, 2. pkt., at erstatningsansvarslovens § 25 kan fraviges for skader, der forvoldes ved udøvelse af offentlig eller erhvervsmæssig virksomhed eller virksomhed, der kan ligestilles hermed.

Det kan ikke antages, at forordningens artikel 82, stk. 5, ændrer på muligheden for – når udgangspunktet i national ret, som i dansk ret, er partsautonomi i inter partes forholdet – at indgå aftaler om den efterfølgende ansvarsfordeling mellem flere erstatningsansvarlige. Dette skyldes navnlig, at forordningens artikel 82, stk. 5, der regulerer spørgsmålet om regres, må anses for at være indsat som en naturlig følge af stk. 4, der fastsætter solidarisk hæftelse. Derudover begrænser en aftale om den efterfølgende ansvarsfordeling ikke muligheden for at sikre fuld erstatning til den registrerede, hvilket er det primære, da en sådan aftale ikke kan afskære den registreredes ret til at rette sit krav mod den eller de erstatningsansvarlige, som den registrerede ønsker at rette kravet imod. Endelig vil det være vanskeligt at tilbyde og yde forsikringsdækning for skade som følge af overtrædelse af forordningens bestemmelser, hvis det i medfør af forordningens artikel 82, stk. 5, ikke var muligt at indgå aftaler om ansvarsbegrænsning.

En sådan adgang til at indgå aftaler om den efterfølgende ansvarsfordeling findes i øvrigt allerede i dansk ret f.eks. i erstatningsansvarslovens § 27, stk. 2, 2. pkt. Et eksempel på en sådan aftale indenfor forordningens område kan være, at en dataansvarlig og en databehandler, forinden en skades indtræden, aftaler, hvordan et ansvar for en eventuel overtrædelse af forordningens artikel 82, stk. 1, skal fordeles.

Det vil med forordningen – ligesom det er tilfældet efter gældende ret – være op til domstolene at vurdere, hvorvidt den erstatningsansvarlige (dataansvarlige eller databehandler), i den givne situation, ifalder et erstatningsansvar som følge af en overtrædelse af forordningens bestemmelser. Som det følger ovenfor, er det dansk rets almindelige erstatningsbetingelser, der finder anvendelse.

Det præciseres i forordningens artikel 82, stk. 4 og 5, at såfremt der er flere erstatningsansvarlige, hæfter de solidarisk med mulighed for regres.

9.6.3.5. Databeskyttelsesforordningens artikel 82, stk. 6

Det følger af forordningens artikel 82, stk. 6, at retssager med henblik på udøvelse af retten til at modtage erstatning anlægges ved de domstole, der er kompetente i henhold til national ret i den medlemsstat, der er omhandlet i artikel 79, stk. 2.

For en nærmere behandling af spørgsmålet om, hvor sager mod en dataansvarlig eller en databehandler kan anlægges, henvises til afsnit 9.3. om effektive retsmidler over for en dataansvarlig eller databehandler, hvoraf det følger, at sager mod en dataansvarlig eller en databehandler anlægges der, hvor denne er etableret, eller der, hvor den registrerede har sit sædvanlige opholdssted.

9.6.4. Overvejelser

Forordningens artikel 82, stk. 1, udvider gældende ret, ved at databehandleren også kan være erstatningsansvarlig. Derudover præciserer bestemmelsen ordlydsmæssigt, at der er ret til erstatning for materiel og immateriel skade, hvilket dog må antages at svare til gældende ret.

Derudover fastsætter forordningens artikel 82, stk. 2, som noget nyt, et erstatningsansvar for databehandlere under nærmere fastlagte omstændigheder, navnlig hvis databehandleren ikke overholder de forpligtelser, som følger af forordningen.

Det præciseres i forordningens artikel 82, stk. 4 og 5, at såfremt der er flere erstatningsansvarlige, hæfter de solidarisk med mulighed for regres.

Det må antages, at medlemsstaternes råderum til at fastsætte egne bestemmelser om erstatningsansvar på persondataområdet med ikrafttrædelsen af forordningen indskrænkes i et vist omfang, da en del af sådanne regler nu følger direkte af forordningens artikel 82.

9.7. Generelle betingelser for pålæggelse af administrative bøder, artikel 83, stk. 1–6

9.7.1. Præsentation

Databeskyttelsesforordningens artikel 83, stk. 1–3, indeholder en række generelle betingelser for pålæggelse af administrative bøder, herunder hvilke principper, der skal iagttages, og hvilke momenter, der har betydning for bødepålæggelse og -størrelse.

Forordningens artikel 83, stk. 4–6, fastlægger, hvilke af forordningens bestemmelser, der pålægges administrative bøder for overtrædelse af og den maksimale bødestørrelse for de pågældende overtrædelser.

9.7.2. Gældende ret

Der er ikke i databeskyttelsesdirektivet taget stilling til spørgsmålet om tilsynsmyndighedernes pålæggelse af administrative bøder, idet det er overladt til medlemsstaterne selv i medfør af artikel 24 at fastsætte sanktioner for overtrædelser af direktivets bestemmelser.

I dansk retspleje er det et grundlæggende princip, at bøder, der har karakter af en strafferetlig sanktion, kun kan pålægges ved domstolene og efter retsplejelovens regler. Datatilsynet har, som tilsynsmyndighed, ikke i dag kompetence til at fastsætte administrative bøder eller til at udstede bødeforelæg, men er henvist til at indgive politianmeldelse, såfremt tilsynet konstaterer overtrædelser af persondataloven. Det følger af Datatilsynets praksis, at tilsynet ofte ikke umiddelbart vil indgive politianmeldelse for et formodet strafbart forhold, men i stedet træffer afgørelse over for den dataansvarlige eller meddeler forbud eller påbud til den pågældende virksomhed mv., hvorefter der ikke foretages politianmeldelse, såfremt virksomheden mv. retter sig herefter og bringer forholdene i orden, medmindre der er tale om grovere eller gentagne brud på persondataloven.[901]

Der er med databeskyttelsesforordningens artikel 83, stk. 9, fra dansk side taget forbehold for, at tilsynsmyndigheden kan pålægge administrative bøder, der har karakter af en strafferetlig sanktion, da dette giver anledning til grundlovsmæssige betænkeligheder efter grundlovens § 3. For en nærmere behandling af spørgsmålet om pålæggelse af bøder for

[901] Persondataloven med kommentarer (2015), s. 661.

overtrædelser af forordningen i Danmark henvises til afsnit 9.10. om administrative bøder i Danmark.

Det følger af en gennemgang af bødeniveauet i Datatilsynets årsberetninger 2008–2010, at overtrædelser af persondataloven straffes med bøder på mellem 2.000 og 25.000 kr., afhængigt af karakteren af de pågældende overtrædelser.[902]

Det er reguleret i persondatalovens § 70, stk. 1 og stk. 2, der vedrører henholdsvis behandling der foretages for private og for offentlige myndigheder, hvilke af bestemmelserne i persondataloven, der er strafpålagte.

Behandling, der foretages for private, er pålagt straf for overtrædelse af en række bestemmelser i medfør af persondatalovens § 70, stk. 1, herunder ved behandling af oplysninger i strid med lovens behandlingsregler, ved overtrædelser af registreredes rettigheder, ved manglende anmeldelse til eller indhentelse af tilladelse fra Datatilsynet. Derudover er overtrædelser af en række bestemmelser pålagt straf i den situation, at Datatilsynet har truffet afgørelse om et forhold, som den dataansvarlige derefter undlader at efterkomme. Endelig fastsætter bestemmelsen straf for at hindre Datatilsynets adgang til oplysninger. For en nærmere behandling af privates strafansvar for overtrædelse af persondatalovens § 70, stk. 1, henvises til afsnit 9.11. om sanktioner.

Behandling, der foretages for offentlige myndigheder, er pålagt straf for overtrædelse af sikkerhedsforanstaltninger og af pligten til at foretage anmeldelse til Datatilsynet af edb-servicevirksomhed, jf. persondatalovens § 70, stk. 2. Derudover kan der pålægges straf for tilsidesættelse af vilkår meddelt af Datatilsynet, om behandling af oplysninger, automatisk registrering af telefonnumre eller overførsel til tredjelande. For en nærmere behandling af strafansvaret for behandling, der foretages for offentlige myndigheder, henvises til afsnit 9.8. om bøder til offentlige myndigheder.

Endelig kan der efter persondatalovens § 70, stk. 3, pålægges straf for behandling, som er undergivet en anden medlemsstats lovgivning, hvis Datatilsynet har truffet en afgørelse, som ikke efterkommes, eller hvis Datatilsynets adgang til oplysninger hindres.

Af en gennemgang af de i § 70 oplistede strafpålagte bestemmelser følger det, at området for, hvornår behandling, der foretages for offentlige myndigheder er strafpålagt er væsentligt indskrænket i forhold til behandling, der foretages for private. Derudover kan det udle-

[902] Persondataloven med kommentarer (2015), s. 663.

des af bestemmelsen, at behandling, der foretages for private er strafpålagt i alle tilfælde, hvor behandling, der foretages for offentlige myndigheder, er strafpålagt.

9.7.3. Databeskyttelsesforordningen

Det fremgår af Kommissionens forslag til databeskyttelsesforordningen, at forordningens artikel 83 (artikel 79 i forslaget) forpligter hver tilsynsmyndighed til at sanktionere de administrative overtrædelser, der er anført i katalogerne ifølge denne bestemmelse og pålægge bøder under hensyntagen til de konkrete omstændigheder i hver sag.[903]

Databeskyttelsesforordningens artikel 83, stk. 1–6, indeholder en række generelle betingelser for pålæggelse af administrative bøder.

Artikel 29-gruppen har om bestemmelserne udtalt, at arbejdsgruppen er tilfreds med, at der indføres større bøder, da det vil give databeskyttelsesmyndighederne mulighed for at udfylde deres rolle som retshåndhævelsesmyndigheder, og da bøderne på grund af deres afskrækkende virkning vil bidrage til, at de dataansvarlige i højere grad opfylder deres forpligtelser. Derudover udtaler Artikel 29-gruppen, at arbejdsgruppen er tilfreds med den harmonisering, der skabes gennem artikel 79 (nuværende artikel 83), som regulerer, hvilke overtrædelser der fører til de højeste bøder, da det vil føre til større konsekvens ved pålæggelse af bøder i hele Den Europæiske Union.[904]

9.7.3.1. Databeskyttelsesforordningens artikel 83, stk. 1.

Det følger af databeskyttelsesforordningens artikel 83, stk. 1, at det er op til tilsynsmyndigheden at sikre at pålæggelse af administrative bøder i henhold til denne artikel for overtrædelse af denne forordning, som omhandlet i stk. 4, 5 og 6, i hver enkelt sag er effektiv, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning.

Det følger bl.a. af præambelbetragtning nr. 148, at pålæggelse af sanktioner, herunder administrative bøder, bør være omfattet af fornødne proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og chartret, herunder effektiv retsbeskyttelse og en retfærdig procedure.

I og med, at tilsynsmyndigheden ikke i Danmark kan pålægge administrative bøder, følger det af bestemmelsen, at det i en dansk udmøntning af denne må sikres, at pålæggelse af bøder i hver enkelt sag er effektiv, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning. For en nærmere behandling af spørgsmålet om en dansk ordning i forhold til pålæggelse af bøder henvises til afsnit 9.10. om administrative bøder i Danmark.

[903] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig, afsnit 3.4.8.
[904] Udtalelse 1/2012 om forslagene til reform af databeskyttelsesreglerne: WP 191, s. 24.

For en nærmere behandling af betydningen af, at sanktionen skal være effektiv, stå i rimeligt forhold til overtrædelsen og have præventiv virkning henvises til afsnit 9.11. om sanktioner, hvoraf det bl.a. følger, at de tre princippers anvendelse på forordningens område præciserer, hvad der allerede følger af gældende ret.

9.7.3.2. Databeskyttelsesforordningens artikel 83, stk. 2.

Det følger af databeskyttelsesforordningens artikel 83, stk. 2, 1. pkt., at afhængigt af omstændighederne i hver enkelt sag pålægges administrative bøder i tillæg til eller i stedet for foranstaltninger som omhandlet i artikel 58, stk. 2, litra a–h og j.

Forordningens artikel 58, stk. 2, litra i, indeholder samtidig en henvisning til artikel 83, hvoraf det følger, at en administrativ bøde kan pålægges i tillæg til eller i stedet for foranstaltningerne i artikel 58, stk. 2, afhængigt af omstændighederne i hvert enkelt tilfælde. Tilsynsmyndighedens korrigerende beføjelser efter artikel 58, stk. 2, begrænser dermed ikke muligheden for at pålægge bøder.

Det følger bl.a. af præambelbetragtning nr. 148, at der, for at *styrke* håndhævelsen af reglerne i denne forordning, bør pålægges sanktioner, herunder administrative bøder, for overtrædelse af denne forordning i tillæg til eller i stedet for passende foranstaltninger, som tilsynsmyndigheden har pålagt i henhold til denne forordning.

Det følger derudover bl.a. af præambelbetragtning nr. 150 at for at *styrke* og harmonisere de administrative sanktioner for overtrædelse af denne forordning, bør hver tilsynsmyndighed have beføjelse til at pålægge administrative bøder, og at pålæggelse af en administrativ bøde eller udstedelse af en advarsel ikke berører anvendelsen af tilsynsmyndighedernes øvrige beføjelser eller andre sanktioner i henhold til denne forordning.

Hvis tilsynsmyndigheden vurderer, at det vil være mest formålstjenligt at pålægge en bøde overfor den dataansvarlige eller databehandleren – og ikke en korrigerende beføjelse efter artikel 58, stk. 2 – skal tilsynsmyndigheden samtidig overveje størrelsen på denne bøde, jf. forordningens artikel 83, stk. 2, 2. pkt. For en nærmere behandling af tilsynsmyndighedens korrigerende beføjelser henvises til afsnit 7.7 om beføjelser.

Databeskyttelsesforordningens artikel 83, stk. 2, 2. pkt., fastsætter, at når der træffes afgørelse om, hvorvidt der skal pålægges en administrativ bøde, og om den administrative bødes størrelse i hver enkelt sag, tages der behørigt hensyn til følgende:

a) overtrædelsens karakter, alvor og varighed under hensyntagen til pågældende behandlings karakter, omfang eller formål samt antal registrerede, der er berørt, og omfanget af den skade, som de har lidt
b) hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt
c) eventuelle foranstaltninger, der er truffet af den dataansvarlige eller databehandleren for at begrænse den skade, som den registrerede har lidt
d) den dataansvarliges eller databehandlerens grad af ansvar under hensyntagen til tekniske og organisatoriske foranstaltninger, som de har gennemført i henhold til artikel 25 og 32
e) den dataansvarliges eller databehandlerens eventuelle relevante tidligere overtrædelser
f) graden af samarbejde med tilsynsmyndigheden for at afhjælpe overtrædelsen og begrænse de negative konsekvenser, som overtrædelsen måtte have givet anledning til
g) de kategorier af personoplysninger, der er berørt af overtrædelsen
h) den måde, hvorpå tilsynsmyndigheden fik kendskab til overtrædelsen, navnlig om den dataansvarlige eller databehandleren har underrettet om overtrædelsen, og i givet fald i hvilket omfang
i) overholdelse af de foranstaltninger, der er omhandlet i artikel 58, stk. 2, hvis der tidligere over for den pågældende dataansvarlige eller databehandler er blevet truffet sådanne foranstaltninger med hensyn til samme genstand
j) overholdelse af godkendte adfærdskodekser i henhold til artikel 40 eller godkendte certificeringsmekanismer i henhold til artikel 42, og
k) om der er andre skærpende eller formildende faktorer ved sagens omstændigheder, såsom opnåede økonomiske fordele eller undgåede tab som direkte eller indirekte følge af overtrædelsen.

Bestemmelsen er en udmøntning af, hvad der følger af præambelbetragtning nr. 148, hvoraf en lignende oplistning fremgår.

Med artikel 83, stk. 2, litra k, fremgår det, at oplistningen ikke er udtømmende, hvorfor eventuelle andre forhold også kan tillægges betydning.

Som det følger af litra i, har tilsynsmyndighedens korrigerende beføjelser efter artikel 58, stk. 2, betydning for fastlæggelsen af, hvordan en overtrædelse af forordningen skal sanktioneres samt en eventuel bødes størrelse. Denne sammenhæng mellem tilsynsmyndighedens korrigerende beføjelser og spørgsmålet om sanktioner medfører, at tilsynsmyndigheden, også i Danmark, i den enkelte sag udtaler sig om, hvorvidt overtrædelser af forordningens bestemmelser efter tilsynsmyndighedernes vurdering skal føre til pålæggelse af bøde.

Bestemmelsen i artikel 83, stk. 2, har en nær sammenhæng med artikel 83, stk. 9, hvoraf det fremgår, at det med den danske ordning med pålæggelse af bøder ved domstolene skal *sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af tilsynsmyndighederne.* En række af de momenter, der følger af oplistningen i artikel 83, stk. 2, tillægges allerede betydning, når anklagemyndigheden/domstolene vurderer, om der er sket overtrædelser af gældende ret. Henset til, at der med forordningen tilstræbes en konsekvent anvendelse af administrative bøder, vil de momenter, der følger af artikel 83, stk. 2, få betydning for spørgsmålet om pålæggelse af bøder.
Bestemmelsen præciserer, hvilke momenter, der skal tillægges betydning, når det skal vurderes, hvordan overtrædelser af forordningens bestemmelser skal sanktioneres, herunder en eventuel bødes størrelse.

9.7.3.3. Databeskyttelsesforordningens artikel 83, stk. 3.
Det følger af databeskyttelsesforordningens artikel 83, stk. 3, at hvis en dataansvarlig eller en databehandler forsætligt eller uagtsomt i forbindelse med de samme eller forbundne behandlingsaktiviteter overtræder flere bestemmelser i denne forordning, må den administrative bødes samlede størrelse ikke overstige beløbet for den alvorligste overtrædelse.

Det følger af bestemmelsen, at der med forordningen er taget stilling til det maksimale bødebeløb, uanset antallet af overtrædelser af forordningen. Dette er antageligvis sket med en forståelse af, at der med forordningen fastsættes betydelige bødebeløb for overtrædelser af forordningens bestemmelser og for at skabe en sikkerhed for niveauet af den bøde, som en dataansvarlig eller en databehandler maksimalt kan pålægges.

Den dataansvarlige eller databehandleren vil dog, uafhængigt af om denne pålægges en bøde på det maksimale niveau, samtidig kunne være erstatningsansvarlig for den skade, der er påført de registrerede ved overtrædelsen af forordningens bestemmelser, hvis betingelserne herfor er opfyldt, ligesom tilsynsmyndigheden stadig vil have mulighed for at træffe korrigerende foranstaltninger.

9.7.3.4. Databeskyttelsesforordningens artikel 83, stk. 4.
Det følger af databeskyttelsesforordningens artikel 83, stk. 4, at overtrædelse af følgende bestemmelser straffes i overensstemmelse med stk. 2 med administrative bøder på op til 10 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 2 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere:

> a) den dataansvarliges og databehandlerens forpligtelser i henhold til artikel 8, 11, 25-39 og 42 og 43

b) certificeringsorganets forpligtelser i henhold til artikel 42 og 43
c) kontrolorganets forpligtelser i henhold til artikel 41, stk. 4.

Det følger bl.a. af præambelbetragtning nr. 148, at denne forordning bør angive overtrædelser og maksimumsbeløb og kriterier for fastsættelse af de tilknyttede administrative bøder, der bør bestemmes af den kompetente tilsynsmyndighed i hvert enkelt tilfælde under hensyntagen til alle relevante omstændigheder i den specifikke situation og med behørig hensyntagen til karakteren, alvoren og varigheden af overtrædelsen og dens konsekvenser og de foranstaltninger, der er truffet for at sikre overholdelse af forpligtelserne i henhold til denne forordning og for at forebygge eller begrænse følgerne af overtrædelsen.

Det følger af præambelbetragtning nr. 150, at når en virksomhed pålægges administrative bøder, forstås en virksomhed i denne forbindelse som en virksomhed som omhandlet i artikel 101 og 102 i TEUF, dvs. EU konkurrencereglerne. Derudover følger det af samme betragtning, at når personer, der ikke er en virksomhed, pålægges administrative bøder, bør tilsynsmyndigheden i forbindelse med fastsættelsen af bødestørrelsen tage hensyn til det generelle indkomstniveau i den pågældende medlemsstat og personens økonomiske situation. Endelig følger det af samme betragtning, at sammenhængsmekanismen også kan anvendes til at fremme konsekvent anvendelse af administrative bøder.

Det EU-retlige virksomhedsbegreb, som præambelbetragtningen henviser til, er udfoldet i retspraksis ved EU-Domstolen. I sag C-437/09 P, AG2R, anførte EU-Domstolen i præmis 41, at inden for EU-konkurrencerettens område omfatter begrebet "virksomhed" "enhver enhed, som udøver økonomisk virksomhed, uanset denne enheds retlige status og dens finansieringsmåde".

For en nærmere behandling af sammenhængsmekanismen henvises til afsnit 8.1. til 8.3. om sammenhæng.

Med forordningen tilsigtes det, at der foretages en harmonisering af reglerne på databeskyttelsesområdet, hvor det er af væsentlig betydning, at der er konsekvens medlemsstaterne imellem på området for pålæggelse af bøder, så det i praksis er uden betydning, i hvilken medlemsstat overtrædelser af forordningens bestemmelser konstateres.

Forordningens artikel 83, stk. 4, pålægger straf for overtrædelse af en række nye tiltag, som ikke kendes fra gældende ret, bl.a. for behandling, der ikke kræver identifikation i artikel 11, for konsekvensanalyser efter artikel 35, for certificering i artikel 42 og for certificeringsorganer i artikel 43. Derudover udvides området for, hvornår en databehandler kan

ifalde strafansvar. Med bestemmelsen sker der en udvidelse af området for de strafpålagte bestemmelser.

9.7.3.5. Databeskyttelsesforordningens artikel 83, stk. 5.

Det følger af databeskyttelsesforordningens artikel 83, stk. 5, at overtrædelse af følgende bestemmelser straffes i overensstemmelse med stk. 2 med administrative bøder på op til 20 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere:

> a) de grundlæggende principper for behandling, herunder betingelserne for samtykke, i artikel 5, 6, 7 og 9
> b) de registreredes rettigheder i henhold til artikel 12-22
> c) overførsel af personoplysninger til en modtager i et tredjeland eller en international organisation i henhold til artikel 44-49
> d) eventuelle forpligtigelser i medfør af medlemsstaternes nationale ret vedtaget i henhold til kapitel IX
> e) manglende overholdelse af et påbud eller en midlertidig eller definitiv begrænsning af behandling eller tilsynsmyndighedens suspension af overførsel af oplysninger i henhold til artikel 58, stk. 2, eller manglende adgang i strid med artikel 58, stk. 1.

De påbud som nævnes i artikel 83, stk. 5, litra e, fremgår af forordningens artikel 58, stk. 2, hvoraf det følger, at tilsynsmyndigheden har beføjelse til at udstede påbud efter artikel 58, stk. 2, litra c, d, e, g og j. Af samme bestemmelse følger det af litra f, at tilsynsmyndigheden har kompetence til midlertidigt eller definitivt at begrænse behandling. Endelig følger det af artikel 58, stk. 1, litra e og f, at tilsynsmyndigheden har beføjelse til at få adgang til oplysninger og til lokaler.

Med artikel 83, stk. 5, sker der en udvidelse af området for de strafpålagte bestemmelser. Dette ses bl.a. ved, at bestemmelserne fastsætter nærmere betingelser for overførsel af personoplysninger til en international organisation i henhold til reglerne i artikel 44–49.

9.7.3.6. Databeskyttelsesforordningens artikel 83, stk. 6.

Det følger af databeskyttelsesforordningens artikel 83, stk. 6, at manglende overholdelse af et påbud fra tilsynsmyndigheden som omhandlet i artikel 58, stk. 2, straffes i overensstemmelse med nærværende artikels stk. 2 med administrative bøder på op til 20 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere.

Der er for så vidt angår påbud fra tilsynsmyndigheden i henhold til forordningens artikel 58, stk. 2, allerede pålagt straf – med samme strafferamme – for overtrædelse heraf i medfør af forordningens artikel 83, stk. 5, litra e.

Det gælder allerede ved fastsættelsen af bøder efter persondatalovens § 70, at bødestørrelsen skal stå i rimeligt forhold til overtrædelsen, men henset til fastsættelsen af et maksimalt bødebeløb, der ligger væsentligt over de bøder, der i dag pålægges, må det antages, at dette vil betyde en væsentlig forøgelse af bødebeløbet også i Danmark, der dog fastsættes af domstolene i hver enkelt sag under hensyn til sagens konkrete omstændigheder.

Det bemærkes, at der også kan fastsættes andre sanktioner for overtrædelser af forordningens bestemmelser i medfør af forordningens artikel 84, herunder sanktionering i form af fængselsstraf.

Forordningen fastsætter – som noget nyt – med artikel 83, stk. 4–6, den maksimale bødestørrelse for overtrædelser af forordningens bestemmelser. De højere bøder for overtrædelser af forordningens bestemmelser vil efter Artikel 29-gruppens vurdering, på grund af bødestørrelsens præventive virkning, være medvirkende til at sikre, at dataansvarlige og databehandlere opfylder deres forpligtelser.[905] Derudover udvider forordningen, hvornår overtrædelser af forordningens bestemmelser kan medføre sanktionering i form af pålæggelse af bøde.

9.7.4. Overvejelser

I og med, at tilsynsmyndigheden ikke i Danmark kan pålægge administrative bøder, følger det af forordningens artikel 83, stk. 1, at det i en dansk udmøntning af denne bestemmelse må sikres, at pålæggelse af bøder i hver enkelt sag er effektiv, står i rimeligt forhold til overtrædelsen og har præventiv virkning

Forordningens artikel 83, stk. 2, præciserer i en dansk kontekst en række af de momenter, som må antages at få betydning for, om overtrædelse af forordningens bestemmelser efter domstolenes vurdering skal føre til pålæggelse af bøde og i givet fald dennes størrelse.

Forordningens artikel 83, stk. 3, fastsætter, at den maksimale bøde i tilfælde af flere overtrædelser ikke kan overstige beløbet for den alvorligste overtrædelse.

Databeskyttelsesforordningens artikel 83, stk. 4–6, fastsætter, som noget nyt, den maksimale bødestørrelse for overtrædelser af forordningens bestemmelser. Derudover udvider

[905] Udtalelse 1/2012 om forslagene til reform af databeskyttelsesreglerne: WP 191, s. 24.

artikel 83 stk. 4 og 5, området for de strafpålagte bestemmelser. Det må antages, at bestemmelsen vil betyde en væsentlig forøgelse af bødestørrelsen for overtrædelser af forordningens bestemmelser i forhold til, hvad overtrædelser af persondataloven i dag takseres til.

9.8. Bøder til offentlige myndigheder, artikel 83, stk. 7

9.8.1. Præsentation

Af databeskyttelsesforordningens artikel 83, stk. 7, følger det, at medlemsstaterne kan fastsætte regler om, hvorvidt og i hvilket omfang en medlemsstats offentlige myndigheder og organer må pålægges administrative bøder.

9.8.2. Gældende ret

Det følger af artikel 24 i databeskyttelsesdirektivet, at medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at dette direktiv gennemføres i fuldt omfang, og at de bl.a. fastsætter de sanktioner, der skal finde anvendelse i tilfælde af overtrædelse af de bestemmelser, der vedtages til dette direktivs gennemførelse.

Af direktivets præambelbetragtning nr. 55 følger det bl.a., at der skal iværksættes sanktioner over for såvel privatretlige som offentlige personer, der overtræder nationale bestemmelser vedtaget med henblik på gennemførelsen af dette direktiv.

Der er med persondatalovens § 70, stk. 1 og 2, der baserer sig på direktivets artikel 24, foretaget en opdeling af de tilfælde, hvor behandling, som udføres for henholdsvis private og offentlige, kan straffes med bøde eller fængsel i indtil 4 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning. Overtrædelse af persondataloven kan begås af både fysiske og juridiske personer, herunder offentlige myndigheder, hvis de generelle betingelser herfor er opfyldt. Strafferammen for overtrædelser af persondataloven er den samme, uanset om behandling udføres for offentlige myndigheder eller private, men overtrædelse af reglerne om behandling af personoplysninger, som udføres for private, er i langt videre omfang strafbelagt end overtrædelse af reglerne om behandlinger, som udføres for offentlige myndigheder.

Registerudvalgets anførte i betænkning nr. 1345, at baggrunden for, at der gælder separate straffebestemmelser for behandling af personoplysninger, der udføres for henholdsvis private og for offentlige myndigheder, bl.a. er, at man havde en tilsvarende ordning i de tidligere gældende registerlove, idet der i bl.a. straffeloven er fastsat en række bestemmelser om tjenesteansvar for personer i offentlig tjeneste eller hverv mv. (se kapitel 16 om forbry-

delser i offentlig tjeneste eller hverv mv., herunder §§ 152-152 f om tavshedspligt), ligesom der også er mulighed for at pålægge offentligt ansatte et disciplinært ansvar.[906]

Det fremgår af bemærkningerne til persondataloven, at passagen "medmindre højere straf er forskyldt efter den øvrige lovgivning" har til formål at sikre, at handlinger, der tillige indebærer en overtrædelse af bestemmelser i anden lovgivning, der kan medføre højere straf, kan henføres under sådanne bestemmelser.[907] Der tænkes herved på bestemmelsen i straffelovens § 264 d om uberettiget videregivelse af oplysninger om en anden persons private forhold. Der tænkes endvidere på forskellige andre bestemmelser i straffeloven om forbrydelser i offentlig tjeneste eller hverv mv., herunder bl.a. §§ 152 og 152 c, d og f samt §§ 155-157.

Persondatalovens § 70, stk. 2, præciserer under hvilke omstændigheder behandling, der udføres for offentlige myndigheder er strafpålagt. Dette er tilfældet, såfremt persondatalovens § 41, stk. 3, eller § 53 overtrædes, eller såfremt vilkår, som nævnt i persondatalovens § 7, stk. 7, § 9, stk. 3, § 10, stk. 3, § 13, stk. 1, § 27, stk. 4, eller en betingelse eller et vilkår for en tilladelse i henhold til regler udstedt i medfør af loven, tilsidesættes. Derudover fastsætter bestemmelsen, at overtrædelser, medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 4 måneder. Der skelnes dermed ikke i bestemmelsen mellem valget af sanktion. Det er domstolene, der i sidste ende tager stilling til, hvorvidt der skal pålægges bøde eller straf i medfør af persondatalovens § 70, stk. 2.

Det følger af bemærkningerne til persondataloven, at det i forbindelse med behandlinger, som foretages for offentlige myndigheder, er fastsat, at der kan pålægges straf for overtrædelse af vilkår, som tilsynsmyndigheden har stillet i henhold til visse bestemmelser, jf. stk. 2. Dette svarer i begrænset omfang til opregningen i lov om offentlige myndigheders registre § 29, stk. 1.[908]

Som eksempel på anvendelsesområdet for persondatalovens § 70, stk. 2, kan nævnes persondatalovens § 41, stk. 3, der er en del af lovens kapitel 11 om behandlingssikkerhed. Bestemmelsen fastsætter, at den dataansvarlige eller databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.

---

[906] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 389.
[907] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 70.
[908] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 70.

9.8.3. Databeskyttelsesforordningen

Det fremgår af databeskyttelsesforordningens artikel 83, stk. 7, at hver medlemsstat, uden at det berører tilsynsmyndighedernes korrigerende beføjelser i henhold til artikel 58, stk. 2, kan fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat.

Det følger af præambelbetragtning nr. 148 at for at styrke håndhævelsen af reglerne i denne forordning, bør der pålægges sanktioner, herunder administrative bøder, for overtrædelse af denne forordning i tillæg til eller i stedet for passende foranstaltninger, som tilsynsmyndigheden har pålagt i henhold til denne forordning.

Det følger af bestemmelsen, at medlemsstaterne ikke ved at fastsætte regler om administrative bøder over for offentlige myndigheders kan ændre på tilsynsmyndighedens korrigerende beføjelser efter artikel 58, stk. 2, hvilket bl.a. vedrører beføjelsen til at udstede advarsler, udtale kritik, begrænsning af eller forbud mod behandling.

Tilsynsmyndigheden har dermed uagtet, hvad der måtte blive bestemt omkring administrative bøder over for offentlige myndigheder, en række beføjelser, der kan anvendes over for private, såvel som over for offentlige myndigheder.

For så vidt angår spørgsmålet om afgrænsning af offentlige myndigheder og organer, jf. artikel 83, stk. 7, er dette nærmere behandlet i afsnit 5.18. om offentlige myndigheder og organers forpligtelse til at udpege en databeskyttelsesrådgiver. Som det fremgår heraf, svarer begrebet til de myndigheder, der henregnes til den offentlige forvaltning efter forvaltningslovens § 1, stk. 1 og 2. Det er således myndigheder omfattet af forvaltningslovens § 1, stk. 1 og 2, der kan blive omfattet af bøder efter artikel 83, stk. 7 og 9, hvis man nationalt i Danmark beslutter sig herfor.

Medlemsstaterne har allerede, i medfør af databeskyttelsesdirektivets artikel 24, som persondatalovens § 70, stk. 2, er baseret på, mulighed for at fastsætte hvilke sanktioner, herunder f.eks. bødestraf, der skal kunne finde anvendelse overfor offentlige myndigheder. Om spørgsmålet bemærkes det, at det er selve den offentlige myndighed, der er strafsubjekt, og at forordningens artikel 83, stk. 7, ikke regulerer ansvaret for ansatte i den offentlige myndighed.

Forordningens artikel 83, stk. 7, præciserer, at det er op til medlemsstaterne at vurdere, om hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat.

9.8.4. Overvejelser

Der vil i forbindelse med vedtagelsen af en ny persondatalov skulle tages stilling til, hvorvidt der skal gives adgang til at pålægge offentlige myndigheder bøder.

9.9. Proceduremæssige garantier, artikel 83, stk. 8

9.9.1. Præsentation

Databeskyttelsesforordningens artikel 83, stk. 8, fastsætter, at tilsynsmyndighedernes udøvelse af beføjelser i henhold til denne artikel skal være underlagt fornødne proceduremæssige garantier i overensstemmelse med EU-retten og medlemsstaternes nationale ret, bl.a. effektive retsmidler og retfærdig procedure.

9.9.2. Gældende ret

Det følger, som nærmere behandlet i afsnit 9.7. om generelle betingelser for pålæggelse af administrative bøder, at det er et grundlæggende princip i dansk retspleje, at bøder, der har karakter af en strafferetlig sanktion, kun kan pålægges ved domstolene og efter retsplejelovens regler. Dette sikrer borgernes retssikkerhed, idet domstolsprocessen sikrer en effektiv beskyttelse af den sigtede.

Af særlig relevans for spørgsmålet om pålæggelse af bøder fastsætter retsplejelovens § 832, stk. 1, en forenklet procedure i sager om lovovertrædelser, der ikke skønnes at ville medføre højere straf end bøde. I medfør af bestemmelsen kan anklagemyndigheden i et bødeforelæg tilkendegive sigtede, at sagen kan afgøres uden retssag, hvis sigtede erklærer sig skyldig i overtrædelsen og erklærer sig rede til inden en nærmere angiven frist at betale en i bødeforelægget angivet bøde. Fristen kan efter anmodning forlænges af anklagemyndigheden.

Såfremt den sigtede ikke erklærer sig skyldig, skal sagen afgøres ved en retssag med de deraf følgende proceduremæssige garantier om mundtlighed, offentlig, objektivitet mv.

For så vidt angår spørgsmålet om effektive retsmidler i chartrets artikel 47 henvises til afsnit 9.2. om adgang til effektive retsmidler over for en tilsynsmyndighed, hvoraf det bl.a. fremgår, at chartrets artikel 47, stk. 1, kodificerer den i EU-retlig retspraksis udviklede pligt for medlemsstaterne til at tilvejebringe den nødvendige adgang til domstolsprøvelse for at sikre en effektiv retsbeskyttelse på de områder, der er omfattet af EU-retten. Det følger endvidere af samme afsnit, at adgangen til domstolsprøvelse i Danmark er betinget af, at sagsøger kan påvise retlig interesse.

Det følger af chartrets artikel 47, stk. 2, at enhver skal have ret til en retfærdig procedure. Af bestemmelsen fremgår det, at enhver skal have ret til en retfærdig og offentlig rettergang inden for en rimelig frist for en uafhængig og upartisk domstol, der forudgående er oprettet ved lov. Bestemmelsen – der finder anvendelse på alle sager om strafferetlig, civilretlig eller administrativ karakter – har et bredere anvendelsesområde end EMRK artikel 6, stk. 1, der også beskytter retten til retfærdig rettergang. Det materielle indhold af artikel 47, stk. 2, skal dog fortolkes i overensstemmelse med EMRK artikel 6, stk. 1.[909]

9.9.3. Databeskyttelsesforordningen

Databeskyttelsesforordningens artikel 83, stk. 8, fastsætter, at tilsynsmyndighedernes udøvelse af beføjelser i henhold til denne artikel skal være underlagt fornødne proceduremæssige garantier i overensstemmelse med EU-retten og medlemsstaternes nationale ret, bl.a. effektive retsmidler og retfærdig procedure.

Forordningens artikel 83, stk. 8, er skrevet med det udgangspunkt, at tilsynsmyndigheden overlades en række beføjelser, som domstolene traditionelt besidder. Tilsynsmyndighederne har imidlertid ikke efter dansk ret mulighed for at pålægge administrative bøder.

Der er fra dansk side med forordningens artikel 83, stk. 9, taget forbehold for, at tilsynsmyndighederne i Danmark efter forordningens ikrafttrædelse ikke skal have beføjelse til at pålægge administrative bøder, da dette giver anledning til grundlovsmæssige betænkeligheder efter grundlovens § 3.

Det er derfor domstolene, der efter dansk ret vil skulle foretage vurderingen af, om der skal pålægges bøde for overtrædelser af forordningens bestemmelser med de deraf følgende proceduremæssige garantier.

9.9.4. Overvejelser

Bestemmelsen er ny for så vidt den forpligter tilsynsmyndigheden til at overholde de fornødne proceduremæssige garantier i forbindelse med udøvelse af dens beføjelser i medfør af artikel 83, hvilket dog er uden betydning i dansk ret.

[909] Jonas Christoffersen, EU's Charter om Grundlæggende Rettigheder med kommentarer, 1. udgave, 2014, s. 421.

9.10. Administrative bøder i Danmark, artikel 83, stk. 9

9.10.1. Præsentation

Det følger af databeskyttelsesforordningens artikel 83, stk. 9, at hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, kan denne artikel anvendes på en sådan måde, at den kompetente tilsynsmyndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem.

9.10.2. Gældende ret

I dansk retspleje er det et grundlæggende princip, at bøder, der har karakter af en strafferetlig sanktion, kun kan pålægges ved domstolene og efter retsplejelovens regler. Denne procedure sikrer borgernes retssikkerhed, idet domstolsprocessen sikrer en effektiv beskyttelse af den sigtede.

Dette skyldes, at det fremgår af grundlovens § 3, at den lovgivende magt er hos kongen (regeringen) og Folketinget i forening, at den udøvende magt er hos kongen (regeringen), og at den dømmende magt er hos domstolene.
Bestemmelsen i grundlovens § 3 må antages at indebære, at lovgivnings-magten ikke i almindelighed kan henlægge behandlingen af strafferetlige bødesager til administrative myndigheder.[910]

Datatilsynet har dermed ikke beføjelse til at fastsætte administrative bøder, som har karakter af en strafferetlig sanktion, men er henvist til at indgive politianmeldelse, såfremt tilsynet konstaterer overtrædelser af persondataloven.

Sager om overtrædelse af persondataloven vil i de fleste tilfælde blive behandlet af anklagemyndigheden på baggrund af en politianmeldelse fra Datatilsynet, såfremt tilsynet konstaterer en mulig strafbar overtrædelse i forbindelse med f.eks. behandlingen af en klage- eller tilsynssag. Datatilsynet vil dog i praksis ofte ikke umiddelbart indgive politianmeldelse for et formodet strafbart forhold, men i stedet træffe afgørelse i forhold til den dataansvarlige eller meddele forbud eller påbud til den pågældende virksomhed mv., hvorefter der – ligesom det tidligere var Registertilsynets faste praksis – ikke foretages politianmeldelse, såfremt virksomheden mv. retter sig herefter og bringer forholdene i orden, medmindre der er tale om grovere eller gentagne brud på persondataloven. Politianmeldelse kan også indgives af private eller af offentlige myndigheder uden om Datatilsynet.[911] Den praktiske behandling af straffesager om overtrædelse af persondataloven foregår således, at

[910] Svar på spørgsmål nr. 1605 af 7. november 2014 fra Folketingets Retsudvalg.
[911] Persondataloven med kommentarer (2015), s. 661.

der i sager, der er anmeldt eller i øvrigt kommet til politiets kendskab uden om vedkommende særmyndighed – hvilket for overtrædelser af persondatalovens vil være Datatilsynet – skal der indhentes en udtalelse fra særmyndigheden, inden der træffes afgørelse om tiltalespørgsmålet.[912]

Fra retpraksis kan der henvises til en sag ved Vestre Landsret (TfK 2010.146 VLD), der handlede om, hvorvidt T Aps videregivelse af billedoptagelser fra en forretnings videokamera i forbindelse med et røveri var en overtrædelse af persondatalovens § 26 a, stk. 1, jf. § 70, stk. 1, nr. 1, jf. § 70, stk. 5.

Datatilsynet indgav den 6. marts 2008 politianmeldelse mod tiltalte, idet Datatilsynet var blevet opmærksom på, at videooptagelser fra tv-overvågning fra tiltaltes forretningslokaler i forbindelse med et røveri den 8. februar 2008 havde været vist på You Tube og været bragt i nyhederne på TV2 Østjylland og i Station 2 Efterlyst på TV2.

Der kan også henvises til en sag ved Datatilsynet, hvor tilsynet på baggrund af en henvendelse fra pressen blev bekendt med, at der på en hjemmeside blev offentliggjort klip fra en overvågningsvideo i forbindelse med et indbrud hos A, hvoraf bl.a. fremgik en person og en bil. Datatilsynet fandt, at det ville være muligt at kunne genkende den person, der optrådte på den offentliggjorte videooptagelse. Af den grund fandt Datatilsynet, at offentliggørelsen var i strid med persondatalovens § 26 a, stk. 1, og pålagde i medfør af persondatalovens § 59, stk. 1, A omgående at ophøre med at offentliggøre billeder fra tv-overvågning af genkendelige personer. Datatilsynet gjorde opmærksom på, at det er strafbart efter persondatalovens § 70, stk. 1, nr. 6, at undlade at efterkomme et påbud meddelt efter § 59. Datatilsynet fandt i øvrigt anledning til at anmode politiet om at foretage en undersøgelse af, i hvilket omfang håndteringen af optagelserne var sket i overensstemmelse med lovgivningen, herunder persondataloven.[913] Dette førte til, at der blev rejst tiltale imod butiksindehaveren, som imidlertid blev frifundet ved byretten i Århus.[914]

Det følger af retsplejelovens § 832, stk. 1, at i sager om lovovertrædelser, der ikke skønnes at ville medføre højere straf end bøde, kan anklagemyndigheden i et bødeforelæg tilkendegive sigtede, at sagen kan afgøres uden retssag, hvis sigtede erklærer sig skyldig i overtrædelsen og erklærer sig rede til inden en nærmere angiven frist at betale en i bødeforelægget angivet bøde.

---

[912] Rigsadvokatmeddelsens afsnit om Særlov – Samarbejdet med særmyndigheder i særlovssager, pkt. 3.2.1., 16. juli 2014.
[913] Sag vedrørende påbud om at stoppe offentliggørelse af billeder fra tv-overvågning, Datatilsynets j.nr. 2008-631-0030.
[914] Persondataloven med kommentarer (2015), s. 430.

Hvis sigtede ikke erklærer sig skyldig i overtrædelsen, kan retsplejelovens § 832, stk. 1, ikke finde anvendelse, hvilket betyder, at sagen må afgøres ved retssag med de deraf følgende proceduremæssige garantier.

Fremgangsmåden med udenretlige bødeforelæg anvendes som udgangspunkt af anklagemyndigheden ved overtrædelser af persondataloven. Det følger af Datatilsynets årsberetning fra 2010, at der, som i tidligere år, også i 2010 har været afsagt enkelte domme og vedtaget enkelte bødeforelæg for overtrædelse af persondataloven.[915] Der er også efter 2010 pålagt straf for overtrædelse af persondataloven.

Om den nærmere behandling af sanktionsformen for overtrædelser af persondataloven i dansk retspraksis henvises til afsnit 9.11. om sanktioner, hvoraf det bl.a. kan udledes, at overtrædelser af persondataloven som altovervejende hovedregel straffes med bøde.

Der er derudover en række offentlige myndigheder, der har en lovhjemlet adgang til at udstede bødeforelæg efter samme procedure som efter retsplejelovens § 832, stk. 1. En sådan adgang følger for fødevaremyndighedernes vedkommende af fødevarelovens § 61 og for skattemyndighedernes vedkommende af skattekontrollovens § 20. Derudover kan Arbejdstilsynet udstede bødeforelæg med hjemmel i en bekendtgørelse herom udstedt i henhold til arbejdsmiljølovens § 82 a.

Der kan også henvises til Advokatnævnet, der i medfør af retsplejelovens § 147 c, har hjemmel til at pålægge en bøde på indtil 300.000 kr., jf. bestemmelsens stk. 1, hvis en advokat, et advokatselskab mv. tilsidesætter de pligter, der følger af retsplejeloven eller af forskrifter fastsat i medfør af loven. Derudover har Revisornævnet hjemmel til at pålægge bøder efter reglerne i revisorlovens § 44.

9.10.3. Databeskyttelsesforordningen

Det følger af forordningens artikel 83, stk. 9, 1. pkt., at hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, kan denne artikel anvendes på en sådan måde, at den kompetente tilsynsmyndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af tilsynsmyndighederne.

Det følger bl.a. af præambelbetragtning nr. 151, at retssystemerne i Danmark og Estland ikke giver mulighed for administrative bøder som fastsat i denne forordning. Reglerne om

[915] Datatilsynets årsberetning 2010, s. 12.

bøder kan i Danmark anvendes ved, at bøder pålægges af de kompetente nationale domstole som en strafferetlig sanktion, forudsat at en sådan anvendelse af reglerne i disse medlemsstater har en virkning, der svarer til virkningen af administrative bøder, som tilsynsmyndighederne i andre lande pålægger. De kompetente nationale domstole bør derfor tage hensyn til en anbefaling fra den hørte tilsynsmyndighed.

Forordningens artikel 83, stk. 9, er en undtagelse til den generelle regel i forordningens artikel 83, stk. 1, hvoraf det fremgår, at tilsynsmyndighederne pålægger administrative bøder.

Det følger af forordningsbestemmelsen, at såfremt der efter national ret ikke er mulighed for, at tilsynsmyndigheden kan pålægge administrative bøder, skal alternativet være, at tilsynsmyndigheden i stedet tager skridt til bøder med tilsvarende virkning.

Artikel 83, stk. 9, er aktuel i en dansk kontekst, jf. umiddelbart ovenfor om gældende ret og svar på spørgsmål nr. 1605 af 7. november 2014 fra Folketingets Retsudvalg.

I en dansk kontekst ses der først og fremmest at være to måder at håndtere artikel 83, stk. 9, på.

Artikel 83, stk. 9, vil for det *første* kunne opfyldes ved, at den kompetente tilsynsmyndighed gives mulighed for at udstede *bødeforelæg* på samme måde som det i dag er tilfældet med fødevaremyndighederne og Arbejdstilsynet. En sådan ordning, hvor tilsynet udsteder bødeforelæg, og hvor domstolene efterfølgende afgør bødespårgsmålet, hvis den, der har begået overtrædelsen, ikke erklærer sig rede til at betale bøden inden en nærmere angivet frist, må opfylde forpligtelsen om, at tilsynsmyndigheden ”tager skridt til” pålæggelse af bøder, jf. artikel 83, stk. 9.

Derudover må forpligtelsen for den kompetente tilsynsmyndighed til at *tage skridt til pålæggelse af bøder* for det *andet* kunne opfyldes ved, at tilsynsmyndigheden på grundlag af de konstaterede overtrædelser af forordningens bestemmelser overvejer, hvorvidt der skal pålægges bøde og i så fald dennes størrelse. Såfremt tilsynsmyndigheden vurderer, at der skal pålægges bøde for de pågældende overtrædelser, indgiver tilsynsmyndigheden *politianmeldelse* sammen med en redegørelse for tilsynsmyndighedens vurdering, herunder niveauet for bøden.

I en sådan ordning vil det derefter være politiet og anklagemyndigheden, der vurderer, hvorvidt man vil gå videre med sagen. Afhængigt af sagens karakter vil politiet/anklagemyndigheden kunne pålægge bøder efter retsplejelovens regler om udenretlige

bødeforelæg. Den sigtede har dog mulighed for ved ikke at erklære sig skyldig at få domstolene til at vurdere sagen.

I de sager, der i dag anmeldes eller kommer til politiet kendskab udenom Datatilsynet, hører politiet Datatilsynet, inden der træffes afgørelse om tiltalespørgsmålet. Denne procedure må antages at kunne indeholdes i betingelsen i artikel 83, stk. 9, om, at tilsynsmyndigheden "tager skridt til bøder" – og vil således kunne opretholdes i en eventuel ny ordning med politianmeldelser, da tilsynet som svar på denne høring, får mulighed for at foretage en vurdering af pålæggelse af bøden samt dennes størrelse.

Forordningen må forstås sådan – bl.a. i lyset af præambelbetragtning nr. 151 – at politiet/anklagemyndigheden, i forbindelse med en eventuel ordning efter artikel 83, stk. 9, der bygger på tilsynets anmeldelse til politiet, er forpligtet til at høre tilsynsmyndigheden inden der træffes afgørelse om tiltalespørgsmålet i sager, der starter med en anmeldelse direkte til politiet, således at tilsynet får lejlighed til at vurdere, om der er grundlag for at tage skridt til bøde. Denne anbefaling skal tillægges vægt, når det skal vurderes, om der skal rejses tiltale.

Det er under alle omstændigheder en forudsætning i forordningens artikel 83, stk. 9, at der ved domstolenes pålæggelse af bøder sikres effektive retsmidler.

Artikel 83, stk. 9, kan næppe antages at indeholde en pligt til at vælge den ene eller anden af de oven for skitserede modeller.

Det kan antages, at det vil være i forordningens "ånd", hvis man i Danmark skaber en national hjemmel til, at tilsynsmyndigheden kan udstede bødeforelæg. Det kan dog som nævnt næppe antages, at der med artikel 83, stk. 9, er et krav om at indføre en sådan ordning med bødeforelæg, i det omfang der indføres en anden ordning med tilsvarende virkning.

Den afgørende forudsætning i forordningens artikel 83, stk. 9, er at virkningen svarer til virkningen af bøder, som administrativt pålægges af tilsynsmyndigheder i andre EU-lande. Den nærmere indretning af systemet er således ikke dikteret i forordningen. Ved en vurdering af, om forordningens bestemmelser overholdes kan man f.eks. måle på en række konkrete momenter, herunder bødestørrelserne og – efter omstændighederne – antallet af bøder. Sådanne oplysninger om bøder i Danmark vil derefter kunne sammenlignes med EU's andre medlemsstater.

Ved udformningen af den danske ordning *skal* det således sikres, at niveauet af bøder svarer til de andre EU-landes. Dette betyder konkret, at der hos den myndighed, der får til

opgave til at udstede bødeforelæg og i øvrigt at føre straffesagerne, skal sikres de fornødne kompetencer og tilstrækkelige ressourcer til, at ordningen medfører, at forordningens bestemmelser overholdes og sanktioneres i samme grad, som vis tilsynsmyndigheden pålagde administrative bøder. Der må i den forbindelse henses til, at der er tale om et kompliceret retsområde, som med forordningen forventeligt vil få større fokus.

Derudover har det også betydning for en vurdering af virkningen, om de momenter, der følger af forordningens artikel 83, stk. 2, tillægges betydning ved vurderingen af, om der skal pålægges bøde og dennes eventuelle størrelse. Domstolene skal tillægge de i bestemmelsen oplistede momenter betydning. For en nærmere behandling af de oplistede momenter, henvises til afsnit 9.7. om generelle betingelser for pålæggelse af administrative bøder.

Af databeskyttelsesforordningens artikel 83, stk. 9, 2. pkt., følger det, at bøder under alle omstændigheder skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. For en nærmere behandling heraf henvises til afsnit 9.11. om sanktioner, hvoraf det bl.a. følger, at de tre princippers anvendelse på forordningens område præciserer, hvad der allerede følger af gældende ret.

Om betydningen af artikel 83, stk. 9, i forhold til spørgsmålet om pålæggelse af bøder over for offentlige myndigheder henvises til afsnit 9.8. herom.

Det følger af artikel 83, stk. 9, 3. pkt., at der gælder en pligt for medlemsstaterne til at meddele Kommissionen om bestemmelserne i deres love, som de vedtager i henhold til dette stykke, senest den 25. maj 2018, og at Kommissionen straks skal underrettes om alle senere ændringslove eller ændringer, der berører dem. Om bestemmelsens nærmere behandling, der ses flere steder i forordningen, henvises til afsnit 9.11. om sanktioner.

9.10.4. Overvejelser

Forordningens artikel 83, stk. 9, fastsætter, at den kompetence tilsynsmyndighed tager skridt til bøder, og at de kompetente nationale domstole pålægger dem. Derudover fastsætter bestemmelsen, at virkningen af den danske ordning skal svare til virkningen af, at tilsynsmyndigheden udstedte administrative bøder, som i andre EU-lande. Der skal sikres de tilstrækkelige kompetencer og tilstrækkelige ressourcer hos den myndighed, der får til opgave at udstede bødeforelæg og i øvrigt føre straffesagerne. Endelig præciserer bestemmelsen, at bøder skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

9.11. Sanktioner, artikel 84

9.11.1. Præsentation

Databeskyttelsesforordningen indeholder i artikel 84, stk. 1, forpligtelser for medlemsstaterne til at fastsætte regler om andre sanktioner, navnlig end pålæggelse af administrative bøder, i tilfælde af overtrædelser af forordningen, samt at medlemsstaterne træffer alle nødvendige foranstaltninger for at sikre, at sanktionerne anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Af artikel 84, stk. 2, følger en underretningspligt for medlemsstaterne til Kommissionen senest den 25. maj 2018 af de bestemmelser, der vedtages i medfør af stk. 1. Derudover følger det, at Kommissionen straks underrettes om alle senere ændringer, der berører nævnte bestemmelser.

9.11.2. Gældende ret

Af databeskyttelsesdirektivets artikel 24 følger det, at medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at dette direktiv gennemføres i fuldt omfang, og de fastsætter bl.a. de sanktioner, der skal finde anvendelse i tilfælde af overtrædelse af de bestemmelser, der vedtages til dette direktivs gennemførelse.

Det følger af direktivets præambelbetragtning nr. 55, at personer, som lider skade som følge af en ulovlig behandling, skal have ret til erstatning fra den dataansvarlige, og at der skal iværksættes sanktioner over for såvel privatretlige som offentlige personer, der overtræder nationale bestemmelser vedtaget med henblik på gennemførelsen af dette direktiv.

EU-Domstolen udtalte i præmis 99 i Lindqvist-dommen[916], 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.

Det er ifølge direktivets artikel 24 op til de enkelte medlemsstater at fastsætte regler om, hvilke sanktioner der skal være forbundet med overtrædelser af nationale bestemmelser om behandling af personoplysninger. Bestemmelsen er i national ret udmøntet ved persondatalovens §§ 70-71, der vedrører bestemmelser om fastsættelse af sanktioner over for behandling, der foretages for private og for offentlige myndigheder. Ved fastsættelsen af sådanne

[916] Sag C-101/01, Lindqvist, dom af 6. november 2003.

sanktioner skal medlemsstaterne opretholde en ligevægt mellem den frie udveksling af personoplysninger og beskyttelsen af privatlivet, jf. også præmis 99 i Lindqvist-dommen.

9.11.2.1. Persondatalovens § 70

I persondatalovens § 70 pålægges offentlige myndigheder og private strafansvar for overtrædelser af specifikke bestemmelser i persondataloven. Det er domstolene, der vurderer, hvorvidt der skal pålægges bøde eller straf for overtrædelser af persondataloven. Datatilsynet har således ikke hjemmel til at pålægge bøder administrativt.

Registerudvalget anførte i betænkning nr. 1345, at det bl.a. i kraft af de nævnte strafbestemmelser i registerlovgivningen samt under hensyntagen til de disciplinærretlige sanktioner, der i øvrigt gælder for ansatte i den offentlige forvaltning, efter udvalgets opfattelse må antages, at den danske lovgivning allerede lever op til bestemmelsen i artikel 24. Der ses derfor ikke at være behov for at fastsætte yderligere straf- og disciplinærretlige foranstaltninger end dem, der allerede gælder til sikring af, at reglerne i lovgivningen overholdes fuldt ud. Det vil dog – som en konsekvens af, at den kommende lovgivning om behandling af personoplysninger mv. vil indeholde en helt ny regulering – skulle overvejes, hvorledes de gældende strafbestemmelser i registerlovgivningen bør revideres.[917]

Der er med persondatalovens § 70, stk. 1 og 2, foretaget en opdeling af de tilfælde, hvor behandling, som udføres for henholdsvis private og offentlige, kan straffes med bøde eller fængsel i indtil 4 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning. Overtrædelse af persondataloven kan dermed begås af både fysiske og juridiske personer, herunder offentlige myndigheder, hvis de generelle betingelser herfor er opfyldt. Straferammen for overtrædelser af persondataloven er den samme uanset, om behandling udføres for offentlige myndigheder eller private, men overtrædelse af reglerne om behandling af personoplysninger, som udføres for private, er i langt videre omfang strafbelagt end overtrædelse af reglerne om behandlinger, som udføres for offentlige myndigheder.

Registerudvalget anførte i betænkning nr. 1345, at baggrunden for, at der gælder separate straffebestemmelser for behandling af personoplysninger, der udføres for henholdsvis private og for offentlige myndigheder, bl.a. er, at man havde en tilsvarende ordning i de tidligere gældende registerlove, idet der i bl.a. straffeloven er fastsat en række bestemmelser om tjenesteansvar for personer i offentlig tjeneste eller hverv mv. (se kapitel 16 om forbrydelser i offentlig tjeneste eller hverv mv., herunder §§ 152-152 f om tavshedspligt), ligesom der også er mulighed for at pålægge offentligt ansatte et disciplinært ansvar.[918]

[917] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 389.
[918] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 389.

Det følger af bemærkningerne til persondataloven, at affattelsen af indledningen til bestemmelserne har til formål at sikre, at handlinger, der tillige indebærer en overtrædelse af bestemmelser, der kan medføre højere straf, kan henføres under sådanne bestemmelser. Der tænkes herved navnlig på bestemmelsen i straffelovens § 264 d om bl.a. forsætlig, uberettiget videregivelse af oplysninger om en anden persons private forhold. Der tænkes endvidere på forskellige andre bestemmelser i straffeloven om forbrydelser i offentlig tjeneste eller hverv mv., herunder bl.a. §§ 152 og 152 c-f samt §§ 155-157.[919]

Sager om overtrædelse af persondataloven vil i de fleste tilfælde blive behandlet af anklagemyndigheden på baggrund af en politianmeldelse fra Datatilsynet, såfremt tilsynet konstaterer en mulig strafbar overtrædelse i forbindelse med f.eks. behandlingen af en klage- eller tilsynssag. Datatilsynet vil dog i praksis ofte ikke umiddelbart indgive politianmeldelse for et formodet strafbart forhold, men i stedet træffe afgørelse i forhold til den dataansvarlige eller meddele forbud eller påbud til den pågældende virksomhed mv., hvorefter der – ligesom det tidligere var Registertilsynets faste praksis – ikke foretages politianmeldelse, såfremt virksomheden mv. retter sig herefter og bringer forholdene i orden, medmindre der er tale om grovere eller gentagne brud på persondataloven. Politianmeldelse kan også indgives af private eller af offentlige myndigheder uden om Datatilsynet.[920]

Rigsadvokaten har ikke udarbejdet retningslinjer, der særligt omhandler behandlingen af straffesager om overtrædelse af persondataloven. Det fremgår imidlertid af Rigsadvokatmeddelelse nr. 6/1994 (revideret 16. juli 2014) om samarbejdet med særmyndigheder i særlovssager, pkt. 3.2.1. om forelæggelse for særmyndigheden, at der i sager, der er anmeldt eller i øvrigt kommet til politiets kendskab uden om vedkommende særmyndighed, skal indhentes en udtalelse fra særmyndigheden, inden der træffes afgørelse om tiltalespørgsmålet.

9.11.2.2. Persondatalovens § 70, stk. 1 – straf til private

Persondatalovens § 70, stk. 1, præciserer under hvilke omstændigheder behandling, der udføres for *private*, er strafpålagt.

Det følger af bemærkningerne til persondataloven, at hvad angår behandlinger, som foretages for private, pålægges der efter stk. 1 strafansvar for overtrædelse af en række af lovens bestemmelser, for undladelse af at efterkomme visse afgørelser truffet af Datatilsynet, for undladelse af at efterkomme tilsynets krav om enhver oplysning, der er af betydning for

[919] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 70.
[920] Persondataloven med kommentarer (2015), s. 661.

dens virksomhed, for at hindre tilsynet i at udøve sin inspektionsbeføjelse, for at tilsidesætte vilkår og lignende eller for at undlade at efterkomme forbud eller påbud. [921]

Derudover følger det af bemærkningerne, at der for så vidt angår straf efter den øvrige lovgivning f.eks. tænkes på straffelovens § 264 d om uberettiget videregivelse af private meddelelser og billeder.

Fra den trykte retspraksis kan nævnes en sag ved Østre Landsret (U 2004.2204 Ø), hvor T, der havde adgang til RKI Kredit information A/S fra sin arbejdsplads, havde indhentet oplysning om A, og derefter videregivet denne, udelukkende til brug for sit lokalpolitiske virke, hvori også A deltog. Landsretten fandt ikke, at indsamlingen af oplysningen var sket til et sagligt formål, eller at der med behandlingen heraf var forfulgt en berettiget interesse. T blev i medfør af persondatalovens § 70, stk. 1, nr. 1, jf. § 5, stk. 2, og § 6, stk. 1, straffet med en bøde på 5.000 kr. med en forvandlingsstraf af fængsel i 8 dage.

Det følger af strafniveauet for overtrædelser af persondataloven, at de sager, der har været om overtrædelse af reglerne om behandling af kreditoplysninger (persondatalovens kapitel 6), typisk er afsluttet med en bøde på 5.000 kr. For så vidt angår uberettiget offentliggørelse på internettet lægges der vægt på karakteren af de offentliggjorte oplysninger. Offentliggørelse af billeder (almindelige oplysninger) har således udløst bøde på 2.000 kr., offentliggørelse af personnumre (fortrolige oplysninger) har udløst bøde på 3.000 kr., og offentliggørelse af helbredsoplysninger (følsomme oplysninger) har udløst bøde på 7.000 kr. I forhold til sager om uberettiget videregivelse af billede og lydoptagelser med personoplysninger, der optages i forbindelse med tv-overvågning i kriminalitetsforebyggende øjemed, er det Datatilsynets praksis som udgangspunkt at anmode anklagemyndigheden om at nedlægge påstand om en bøde på minimum 5.000 kr. På markedsføringsområdet er der givet bøder på henholdsvis 7.000 kr., 7.500 kr. og 25.000 kr. Hvad endelig angår private virksomheders ulovlige behandling af følsomme personoplysninger, er sagerne afgjort med bøder på henholdsvis 5.000 kr. og 10.000 kr.[922]

9.11.2.3. Persondatalovens § 70, stk. 2 – straf til offentlige myndigheder

Persondatalovens § 70, stk. 2, præciserer under hvilke omstændigheder behandling, der udføres for offentlige myndigheder, er strafpålagt. Dette er tilfældet, såfremt persondatalovens § 41, stk. 3, eller § 53 overtrædes, eller såfremt vilkår, som nævnt i persondatalovens § 7, stk. 7, § 9, stk. 3, § 10, stk. 3, § 13, stk. 1, § 27, stk. 4, eller en betingelse eller et vilkår

[921] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 70.

[922] Persondataloven med kommentarer (2015), s. 663, der refererer til Datatilsynets årsberetninger fra 2008 – 2010.

for en tilladelse i henhold til regler udstedt i medfør af loven, tilsidesættes. Derudover fastsætter bestemmelsen, at overtrædelser, medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 4 måneder. Der skelnes dermed ikke i bestemmelsen mellem valget af sanktion. Det er domstolene, der i sidste ende tager stilling til, hvorvidt der skal pålægges bøde eller straf i medfør af persondatalovens § 70, stk. 2. Det bemærkes i den forbindelse, at der dog – efter omstændighederne – kan pålægges offentligt ansatte andre sanktioner, herunder disciplinære sanktioner.

Det følger af bemærkningerne til persondataloven, at det i forbindelse med behandlinger, som foretages for offentlige myndigheder, er fastsat, at der kan pålægges straf for overtrædelse af vilkår, som tilsynsmyndigheden har stillet i henhold til visse bestemmelser, jf. stk. 2.[923]

Strafansvaret for offentlige myndigheder som sådan er imidlertid undergivet den begrænsning, der følger af den generelle bestemmelse i straffelovens § 27, stk. 2. Efter denne bestemmelse kan statslige myndigheder og kommuner alene straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private.

9.11.2.4. Persondatalovens § 70, stk. 3

Persondatalovens § 70, stk. 3, præciserer under hvilke omstændigheder behandling, som er undergivet en anden medlemsstats lovgivning, er strafpålagt.

Det følger af bemærkningerne, at der efter bestemmelsen i stk. 3 kan pålægges straf i forbindelse med behandlinger, som er omfattet af en anden medlemsstats lovgivning, men som Datatilsynet efter § 64, stk. 1, påser lovligheden af. Med bestemmelsen sikres det, at der vil kunne pålægges databehandlere strafansvar, hvis de ikke efterlever tilsynets påbud eller forbud efter § 59, hvis de ikke opfylder tilsynets krav efter 62, stk. 1, eller hvis de hindrer tilsynet i at udføre inspektioner, jf. § 62, stk. 3 og 4.[924]

9.11.2.5. Persondatalovens § 70, stk. 4

Persondatalovens § 70, stk. 4, fastsætter, at der for regler, der udstedes i medfør af loven, kan fastsættes straf af bøde eller fængsel indtil 4 måneder. Det følger af bemærkningerne

[923] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 70.
[924] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 70.

til persondataloven, at bestemmelsen svarer til lov om private registre § 27, stk. 2, og at den afløser lov om offentlige myndigheders registre § 29, stk. 2.[925]

9.11.2.6. Persondatalovens § 70, stk. 5

Persondatalovens § 70, stk. 5, fastsætter, at der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel (der vedrører juridiske personers strafansvar).

Af straffelovens § 25 følger det, at en juridisk person kan straffes med bøde, når det er bestemt ved eller i medfør af lov. Af den grund er det nødvendigt med en selvstændig bestemmelse i persondataloven der fastsætter, at juridiske personer kan straffes med bøde.

Af straffelovens § 26 følger det, at enhver juridisk person er omfattet, herunder aktie-, anparts- og andelsselskaber, interessentskaber, foreninger, fonde, boer, kommuner og statslige myndigheder.

Fra trykt retspraksis kan nævnes en sag ved Østre Landsret (U 2007.334 Ø), hvor T A/S havde indlagt en salgsopstilling, på en hjemmeside på internettet om tvangsauktioner, hvori 2 personers cpr-numre i en periode på 7 dage var anført flere steder. T A/S idømtes en bøde på 3.000 kr. efter persondatalovens § 70, stk. 5, jf. stk. 1, nr. 1, jf. § 11, stk. 3.

9.11.2.7. Persondatalovens § 71

Persondatalovens § 71 fastsætter, at den der driver eller er beskæftiget med virksomhed som nævnt i § 59, stk. 1, nr. 2-5, eller § 53, ved dom for strafbart forhold kan frakendes retten hertil, såfremt det udviste forhold begrunder en nærliggende fare for misbrug. I øvrigt finder straffelovens § 79, stk. 3 og 4, anvendelse.

Det følger af bemærkningerne til persondataloven, at bestemmelsen afløser reglen i lov om private registre § 28 om frakendelse af retten til at drive eller beskæftige sig med kreditoplysningsbureauvirksomhed, advarselsregistre og edb-servicebureauer. Bestemmelsen gælder imidlertid også for personer, som erhvervsmæssigt yder bistand ved stillingsbesættelse samt personer, som fører retsinformationssystemer. Straffelovens bestemmelser om tidsmæssig begrænsning af frakendelsen af retten og om umiddelbar udelukkelse af denne under sagens behandling mv. finder tillige anvendelse.[926]

[925] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 70.

[926] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 71.

9.11.3. Databeskyttelsesforordningen

9.11.3.1. Databeskyttelsesforordningens artikel 84, stk. 1

Databeskyttelsesforordningen indeholder i artikel 84, stk. 1, regler om, at medlemsstaterne fastsætter andre sanktioner, der skal anvendes i tilfælde af overtrædelser af forordningen, navnlig overtrædelser, som ikke er underlagt administrative bøder i henhold til artikel 83, samt at medlemsstaterne træffer alle nødvendige foranstaltninger for at sikre, at sanktionerne anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Det følger bl.a. af præambelbetragtning nr. 148, at der, for at styrke håndhævelsen af reglerne i denne forordning, bør pålægges sanktioner, herunder administrative bøder, for overtrædelse af denne forordning i tillæg til eller i stedet for passende foranstaltninger, som tilsynsmyndigheden har pålagt i henhold til denne forordning. Det følger derudover af betragtningen, at pålæggelse af sanktioner, herunder administrative bøder, bør være omfattet af fornødne proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og chartret, herunder effektiv retsbeskyttelse og en retfærdig procedure.

Det følger af præambeltragtning nr. 149, at medlemsstaterne bør kunne fastsætte regler om strafferetlige sanktioner for overtrædelse af denne forordning, herunder for overtrædelse af nationale regler vedtaget i henhold til og inden for rammerne af denne forordning. Disse strafferetlige sanktioner kan også åbne mulighed for fratagelse af den opnåede fortjeneste ved overtrædelse af denne forordning. Pålæggelse af strafferetlige sanktioner for overtrædelse af sådanne nationale regler og administrative sanktioner bør dog ikke føre til et brud på ne bis in idem-princippet (forbud mod dobbelt straf) som fortolket af Domstolen.

Derudover følger det af præambelbetragtning nr. 152, at når denne forordning ikke harmoniserer administrative sanktioner eller om nødvendigt i andre tilfælde, f.eks. i tilfælde af alvorlige overtrædelser af denne forordning, bør medlemsstaterne indføre en ordning, der giver mulighed for at pålægge sanktioner, som er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning. Sanktionernes art, strafferetlig eller administrativ, bør fastsættes i medlemsstaternes nationale ret.

Ordlyden af forordningens artikel 84, stk. 1, svarer delvist til ordlyden af databeskyttelsesdirektivets artikel 24. Begge bestemmelser forpligter medlemsstaterne til at fastsætte *nødvendige foranstaltninger* henholdsvis til, at direktivet gennemføres og til, at sanktionerne fastsat i medfør af forordningen anvendes.

Direktivet tager alene på det generelle plan stilling til spørgsmålet om fastlæggelse af sanktioner, men overlader det til medlemsstater at bestemme, hvordan og i hvilket omfang overtrædelser af direktivets bestemmelser skal sanktioneres.

Nyt er det, at det af forordningens artikel 84 følger, at medlemsstaterne navnlig bør sanktionere de overtrædelser, der ikke er omfattet af forordningens artikel 83. Heri må forstås, at medlemsstaterne omvendt ikke er udelukket fra at fastsætte andre sanktioner for overtrædelser af de bestemmelser, som i forordningen straffes med administrative bøder. Denne forståelse støttes bl.a. af præambelbetragtning nr. 149, hvorefter medlemsstaterne skal sikre, at der ikke ved fastsættelsen af andre sanktioner sker en overtrædelse af forbuddet mod dobbelt straf. Et eksempel på en sådan anden sanktion, kan, udover bøde- og fængselsstraf, være frakendelse af retten til at drive en bestemt virksomhed.

For en nærmere behandling af de generelle betingelser for pålæggelse af administrative bøder henvises til afsnit 9.7. herom.

Endelig præciseres det i forordningen, at sanktionerne er underlagt en række principper. Det følger, at sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen (proportionalitet) og have afskrækkende virkning. Udover ekspliciteringen medfører de tre principper ikke ændringer i forhold til gældende ret, da det antages, at medlemsstaterne allerede i forbindelse med fastsættelse af sanktioner har skullet sikre sig overholdelsen af et effektivitets-, et proportionalitets- og et afskrækkelsesprincip. Sådanne principper følger generelt af EU-retten og kan læses ind i direktivets krav om, at medlemsstaterne *træffer de nødvendige foranstaltninger for at sikre, at dette direktiv gennemføres i fuldt omfang*.

Det følger af bestemmelsen, at medlemsstaterne er overladt et vidt skøn til at vurdere, hvorvidt, og i så fald hvordan, overtrædelser af forordningens bestemmelser skal sanktioneres, i det omfang, der ikke i forordningen er taget stilling hertil.

I det omfang, der nationalt fastsættes regler om andre sanktioner, herunder bøde- og fængselsstraf, følger det af præambelbetragtning nr. 149, at dette ikke må føre til en overtrædelse af forbuddet mod dobbelt straf som fortolket af EU-Domstolen. Nationale regler om sanktionering skal allerede efter gældende ret sikre mod dobbelt straf, hvilket bl.a. følger af artikel 4 i Tillægsprotokol 7 til Den Europæiske Menneskerettighedskonvention (EMRK), og af artikel 50 i EU's Charter for Grundlæggende Rettigheder.

9.11.3.2. Databeskyttelsesforordningens artikel 84, stk. 2

Af artikel 84, stk. 2, følger en underretningspligt for medlemsstaterne til Kommissionen senest den 25. maj 2018 af de bestemmelser, der vedtages i medfør af stk. 1. Derudover

følger det, at Kommissionen straks underrettes om alle senere ændringer, der berører nævnte bestemmelser.

Det må antages, at der med forpligtelsen til, at medlemsstaterne *straks* underretter Kommissionen om alle senere ændringer, der berører nævnte bestemmelser, menes, at dette skal ske hurtigst muligt, hvilket for Danmarks vedkommende vil kunne ske ved, at Kommissionen orienteres, når ændringsforslaget er vedtaget af Folketinget.

9.11.3.3. Databeskyttelsesforordningen i en dansk kontekst

Det følger af artikel 84, stk. 1, 1. pkt., at medlemsstaterne skal fastsætte regler om andre sanktioner, herunder bøde- eller fængselsstraf, for overtrædelser af denne forordning, navnlig overtrædelser, som ikke er underlagt administrative bøder efter forordningens artikel 83. Det bemærkes i den forbindelse, at sådan mulighed f.eks. eksisterer for nationalt at pålægge bødestraf for overtrædelse af forordningens artikel 10, der ikke ses at være omfattet af forordningens artikel 83.

I den forbindelse bemærkes ligeledes, at det følger af forordningens artikel 83, stk. 5, litra d, at overtrædelse af eventuelle forpligtelser i medfør af medlemsstaternes nationale ret vedtaget i henhold til kapitel IX straffes med administrative bøder, hvilket bl.a. omfatter retten til ytringsfrihed, artikel 85, og behandling af personoplysninger i forbindelse med ansættelsesforhold, artikel 88.

I samme forbindelse bemærkes også, at det også følger af forordningens artikel 83, stk. 6, at manglende overholdelse af påbud fra tilsynsmyndigheden som omhandlet i artikel 58, stk. 2, straffes med administrative bøder. Det følger bl.a. af artikel 58, stk. 2, litra d, at tilsynsmyndigheden kan give den dataansvarlige eller databehandleren påbud om at bringe behandlingsaktiviteter i overensstemmelse med bestemmelserne i *denne forordning*. Sådanne bestemmelser må antageligvis også omfatte bestemmelser i særlovgivning, vedtaget i henhold til denne forordning, hvis overtrædelse er sanktioneret.

Det fremgår derudover af forordningens artikel 84, stk. 1, 1. pkt., at det "*navnlig* [er] overtrædelser, som ikke er underlagt administrative bøder i henhold til artikel 83", hvor medlemsstaterne fastsætter andre sanktioner end administrative bøder efter artikel 83. Heraf må det kunne udledes, at der også kan indføres eller opretholdes nationale bestemmelser, vedtaget indenfor forordningens rammer, om pålæggelse af bøde- og fængselsstraf, som strafferetlige sanktioner, selvom overtrædelse af den nationale bestemmelse i princippet også er omfattet af artikel 83.

Denne fortolkning støttes af præambelbetragtning nr. 149, hvoraf det bl.a. følger, at medlemsstaterne bør kunne fastsætte regler om strafferetlige sanktioner for overtrædelse af denne forordning, *herunder* for overtrædelse af nationale regler vedtaget i henhold til og inden for rammerne af denne forordning. Endelig støttes fortolkningen af, at der må være forskel på at pålægge en administrativ bøde som omhandlet i forordningens artikel 83, og på at pålægge en bødestraf, som en strafferetlig sanktion, efter forordningens artikel 84, jf. også præambelbetragtning nr. 152. Det kan heraf udledes, at der overlades medlemsstaterne en vis manøvremargin for fastsættelse af sanktioner, herunder også til at fastsætte bødestraf for overtrædelse af national særlovgivning inden for rammerne af forordningen. Dette betyder, at man nationalt kan indføre og opretholde bestemmelser i særlovgivning, der straffes med bøde, fængsel eller andre sanktioner.

Et eksempel på en sådan bestemmelse, der kan opretholdes, findes i straffelovens § 264 d om uberettiget videregivelse af meddelelser eller billeder vedrørende en andens private forhold eller i øvrigt billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget offentligheden, der straffes med bøde eller fængsel indtil 6 måneder.

Når det af forordningens artikel 84, stk. 1, 2. pkt., følger, at sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning, må det for fastsættelse af sanktioner for overtrædelser af sådanne nationale særregler, antages, at sanktionerne skal fastsættes forholdsmæssigt i forhold til bødeniveauet i forordningens artikel 83 for herved at sikre en virkning svarende til forordningens.

9.11.4. Overvejelser

Artikel 84, stk. 1, 1. pkt., fastsætter som noget nyt, at medlemsstaterne navnlig skal sanktionere de overtrædelser, der ikke er omfattet af forordningens artikel 83. Bestemmelsen overlader dog medlemsstaterne en vis manøvremargin for fastsættelse af sanktioner indenfor forordningens rammer. Dette betyder bl.a., at man – i medfør af bestemmelsen – nationalt kan indføre og opretholde bestemmelser i særlovgivning, der straffes med andre sanktioner, herunder bøde- eller fængselsstraf.

Derudover præciseres det i forordningens artikel 84, stk. 1, 2. pkt., at sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Der vil i forbindelse med vedtagelsen af en ny persondatalov skulle tages stilling til, i hvilket omfang den gældende sanktionering skal videreføres.

10. Forordningens kapitel IX: Bestemmelser vedrørende specifikke behandlingssituationer

10.1. Rammerne i artikel 85 vedrørende ytrings- og informationsfrihed

10.1.1. Præsentation

Det understreges i persondatalovens § 2, stk. 2, at persondataloven ikke finder anvendelse, hvis det er i strid med retten til informations- og ytringsfrihed, jf. Den Europæiske Menneskerettighedskonvention artikel 10.

Endvidere følger det af persondatalovens § 2, stk. 5-9, at visse behandlinger af personoplysninger i vidt omfang er undtaget fra store dele af lovens område som følge af hensynet til ytringsfrihed. Bestemmelserne er baseret på artikel 9, i databeskyttelsesdirektivet, hvorefter medlemsstaterne fastsætter undtagelser fra direktivet, som er nødvendige for at forene retten til privatlivets fred med reglerne om ytringsfrihed.

Databeskyttelsesforordningen indeholder en tilsvarende bestemmelse i artikel 85, hvorefter medlemsstaterne fastsætter undtagelser fra forordningens bestemmelser, hvis det er nødvendigt for at forene retten til beskyttelse af personoplysninger med ytrings- og informationsfriheden.

10.1.2. Gældende ret

10.1.2.1. Persondatalovens § 2, stk. 2

Det fremgår 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.

Det fremgår af bemærkningerne til persondataloven[927], 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 artikel 10 i Den Europæiske Menneskerettighedskonvention.

Det fremgår endvidere af bemærkningerne til loven, at det er en selvfølge, at persondataloven i øvrigt administreres således, at der ikke handles i strid med Danmarks internationale forpligtelser, herunder artikel 10 og de øvrige bestemmelser i Den Europæiske Menneskerettighedskonvention.

[927] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 2.

Den Europæiske Menneskerettighedskonvention repræsenterer et grundlæggende værdisæt, som EU-Domstolen lægger til grund ved fortolkningen af EU-regler.[928] I sag C-101/01, Lindqvist, dom af 6. november 2003, tog EU-Domstolen bl.a. stilling til spørgsmålet om, hvorvidt reglerne i databeskyttelsesdirektivet i den konkrete sag medførte begrænsninger, der var i strid med det almindelige princip om ytringsfrihed e1ler andre friheder og rettigheder, svarende til bl.a. Den Europæiske Menneskerettighedskonventions artikel 10.[929]

EU-Domstolen udtalte i sagen, at bestemmelserne i direktivet ikke i sig selv medfører en begrænsning, der er i strid med det almindelige princip om ytringsfrihed eller andre friheder og rettigheder, der er gældende inden for EU, og som svarer til bl.a. Den Europæiske Menneskerettighedskonventionens artikel 10. Herudover udtalte domstolen, at det påhviler de nationale myndigheder og domstole, der skal anvende de nationale bestemmelser til gennemførelse af direktivet, at sikre en retfærdig ligevægt mellem de omhandlede rettigheder og interesser, herunder de grundlæggende rettigheder, der beskyttes ved fællesskabets retsorden.[930]

Selve anvendelsen af persondatalovens § 2, stk. 2, beror på et konkret skøn, hvor der på den ene side skal lægges vægt på hensynet til informations- og ytringsfriheden, samtidig med at bestemmelsen ikke må føre til en udhuling af den beskyttelse af privatlivets fred, som er formålet med persondataloven.[931]

Fra Datatilsynets praksis kan bl.a. nævnes sagen om en kommunes klage over en hjemmeside, som offentliggjorde oplysninger om bl.a. navngivne kommunale medarbejdere.[932] Formålet med hjemmesiden var at registrere diverse personer, der efter visse borgeres mening havde overtrådt lovgivningen, eller hvis de pågældende borgere havde følt sig uretfærdigt behandlet. Det fremgik af hjemmesiden, at registreringen de pågældende personer på hjemmesiden ikke nødvendigvis var ensbetydende med, at den pågældende var dømt eller sigtet for nogle af de anførte forhold, men at registreringen kunne skyldes, at en borger havde følt sig uretfærdigt behandlet af den pågældende.

Efter klage fra en kommune fandt Datatilsynet ikke grundlag for at foretage sig noget i sagen – på baggrund af lovens § 2, stk. 2. Tilsynet lagde bl.a. vægt på, at hjemmesiden var præget af subjektive vurderinger og værdiladede ytringer, og at oplysningerne indgik som en del af meningstilkendegivelserne, hvilket måtte stå klar for brugerne af hjemmesiden.

[928] Persondataloven med kommentarer (2015), s. 109.
[929] Sag C-101/01, Lindqvist, præmis nr. 18, 6.
[930] Sag C-101/01, Lindqvist, præmis nr. 90.
[931] Persondataloven med kommentarer (2015), s. 111.
[932] Datatilsynets j.nr. 2011-215-0874.

En anden kommune anmodede efterfølgende Datatilsynet om på ny at tage stilling til hjemmesiden.[933] Den pågældende kommune henviste til, at det nu ved dom over indehaveren af hjemmesiden var slået fast, at oplysningerne på hjemmesiden indebar en overtrædelse af straffelovens § 267 om ærekrænkelse og § 268 om bagvaskelse, ligesom at ejeren af hjemmesiden ved dommen var forpligtet til at fjerne visse oplysninger om nogle navngivne personer fra hjemmesiden. Datatilsynet fandt fortsat ikke grundlag for at gå ind i sagen, idet det stadig var tilsynets vurdering, at behandlingen af personoplysninger på hjemmesiden ikke var omfattet af persondataloven, jf. lovens § 2, stk. 2.

I en række andre sager har Datatilsynet udvist tilbageholdenhed med anvendelse af persondatalovens § 2, stk. 2, f.eks. ved vurdering af hjemmesider, hvor flere indlæg fremstod som beskrivelser af faktuelle forhold og ikke nødvendigvis (udelukkende) som meningstilkendegivelser.

Datatilsynet har i to sager[934] taget stilling til spørgsmål om lovligheden af offentliggørelse af oplysninger på en hjemmeside, der i sit indhold og opbygning mindede meget om den ovenfor omtalte hjemmeside.

Hjemmesiden, hvis tema var forholdet mellem borgere og myndigheder/beslutningstagere, var i høj grad præget af subjektive vurderinger og værdiladede ytringer. Formålet med hjemmesiden var angiveligt bl.a., at "bekæmpe magtmisbrug, korruption og svindel inden for det offentlige og opnå retfærdighed i samfundet". Et andet formål var at skabe debat, idet der var adgang til et debatforum på hjemmesiden. Endvidere fremgik det, at hjemmesideindehaveren gerne hjalp personer, der har været udsat for overgreb.

I modsætning til den ovenfor omtalte hjemmeside indeholdt hjemmesiden imidlertid ingen forbehold med hensyn til rigtigheden af oplysningerne på siden. Datatilsynet fandt på den baggrund, at persondatalovens § 2, stk. 2, ikke fandt anvendelse, men at offentliggørelse af personoplysninger måtte vurderes efter persondatalovens regler under inddragelse af hensynet til informations- og ytringsfriheden.

Endelig skal det bemærkes, at det endvidere er Datatilsynets praksis, at § 2, stk. 2, som udgangspunkt ikke kan føre til, at der kan offentliggøres følsomme oplysninger omfattet af § 7 og § 8.[935]

[933] Datatilsynets j.nr. 2014-222-0049.
[934] Datatilsynets j.nr. 2014-217-0783 og 2014-217-0878.
[935] Persondataloven med kommentarer (2015), s. 112.

10.1.2.2. Databeskyttelsesdirektivets artikel 9

Det fremgår af artikel 9 i databeskyttelsesdirektivet, at medlemsstaterne i forbindelse med behandling af personoplysninger, der udelukkende finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed, kun fastsætter fritagelser eller undtagelser fra bestemmelserne i visse dele af direktivet, for så vidt som de er nødvendige for at forene retten til privatlivets fred med reglerne for ytringsfrihed.

Det fremgår endvidere af artikel 9, at der kan fritages eller undtages fra bestemmelserne i direktivets kapitel II om almindelige betingelser for lovlig behandling af personoplysninger, kapitel IV om videregivelse af personoplysninger til tredjelande og kapitel VI om tilsynsmyndighed samt gruppe til beskyttelse af personer i forbindelse med behandling af personoplysninger.

Registerudvalget anførte i betænkning nr. 1345, at der på baggrund af direktivets artikel 9 skal foretages en afvejning af, hvilke fritagelser eller undtagelser fra reglerne i de angivne kapitler i direktivet, som er nødvendige i dansk ret for at forene retten til privatlivets fred med reglerne om ytringsfrihed.[936]

Dette er afspejlet i persondatalovens §§ 2, stk. 5-9, som indebærer, at visse behandlinger af personoplysninger i vidt omfang er undtaget fra store dele af lovens område som følge af hensynet til ytringsfrihed.

10.1.2.3. Persondatalovens § 2, stk. 5-8

Det fremgår af persondatalovens § 2, *stk. 5*, at loven ikke finder anvendelse på behandlinger, der er omfattet af lov om massemediers informationsdatabaser. Dette indebærer, at visse behandlinger af personoplysninger, som foretages af medierne, i stedet er omfattet af de særlige, mere lempelig regulering i henhold til lov om massemediers informationsdatabaser.[937]

Dernæst fremgår det af persondatalovens § 2, *stk. 6*, at loven heller ikke finder anvendelse på 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 dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.

Det fremgår endvidere af persondatalovens § 2, *stk. 7*, at det samme gør sig gældende for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte tekster,

[936] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 208.
[937] Persondataloven med kommentarer (2015), s. 121.

billeder og lydprogrammer, der omfattes af medieansvarslovens § 1, nr. 3, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelse.

Lovens § 2, *stk. 6* og *7*, omhandler således de såkaldte uredigerede fuldtekstdatabaser, som er undtaget fra både lov om massemediers informationsdatabaser og persondataloven, og derfor som udgangspunkt er reguleret af medieansvarsloven.[938] Fælles for persondatalovens §§ 2, *stk. 6* og *7* er, at lovens §§ 41, 42 om behandlingssikkerhed og 69 om erstatning ved overtrædelse af reglerne om behandlingssikkerhed finder anvendelse.

Persondatalovens § 2, *stk. 8*, er begrænset til at omfatte manuelle arkiver over udklip fra offentliggjorte, trykte artikler, som udelukkende behandles i journalistisk øjemed. Det betyder, at arkiver, der ikke udelukkende anvendes i journalistisk øjemed, i sin helhed vil være omfattet af persondatalovens regler.[939] Det skal hertil bemærkes, at visse private samlinger helt kan undtages efter persondatalovens § 2, stk. 3. Der henvises i den forbindelse til afsnit 2.2. om aktiviteter af rent privat karakter.

Det fremgår endvidere af bestemmelsen, at reglerne i persondatalovens § 41-42 og 69 finder anvendelse for journalisters manuelle arkiver over presseklip.

10.1.2.4. Persondatalovens § 2, stk. 9

Det fremgår af persondatalovens § 2, stk. 9, *1. pkt.*, at behandling af oplysninger, som i øvrigt udelukkende finder sted i journalistisk øjemed, alene er omfattet af bestemmelserne i lovens §§ 41 og 42 om behandlingssikkerhed og 69 om erstatning ved overtrædelse af reglerne om behandlingssikkerhed.

Det fremgår af bemærkningerne til persondataloven[940], at § 2, stk. 9, *1. pkt.*, tager sigte på den elektroniske behandling af personoplysninger, som udelukkende foretages som led i journalistisk virksomhed i forbindelse med udarbejdelse af artikler mv. under anvendelse af almindelige tekstbehandlingssystemer.

Det fremgår endvidere af lovens § 2, stk. 9, *2. pkt.*, at det samme gælder for behandling af oplysninger, som udelukkende sker med henblik på kunstnerisk eller litterær virksomhed.

For så vidt angår § 2, stk. 9, *2. pkt.*, fremgår det af bemærkningerne, at lovens regler ligeledes kun i begrænset omfang finder anvendelse på behandling, som udelukkende sker med henblik på kunstnerisk eller litterær virksomhed. Med udtrykket *litterær virksomhed* sigtes

[938] Persondataloven med kommentarer (2015), s. 121.
[939] Persondataloven med kommentarer (2015), s. 123.
[940] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 2, stk. 10 (nuværende stk. 9).

– ifølge bemærkningerne til bestemmelsen – til ”skønlitterær virksomhed”, f.eks. udarbejdelse af nøgleromaner.

Hertil skal det bemærkes, at Datatilsynet i en udtalelse har antaget, at persondatalovens § 2, stk. 9, *2. pkt.*, også omfatter faglitterære bøger.[941] Dog vil behandling af oplysninger i forbindelse med sædvanlige forskningsaktiviteter ikke kunne undtages efter persondatalovens § 2, stk. 9.[942]

Fælles for behandling i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed er, at § 2, *stk. 9*, alene gælder for behandling som *udelukkende* finder sted til disse formål.

Det fremgår af bemærkningerne til loven, at hvis behandlingen ikke kan anses for udelukkende at ske til de nævnte formål, finder persondatalovens regler fuldt ud anvendelse på denne behandling. Det er Datatilsynet, som fører tilsyn med, om en behandling udelukkende sker i de nævnte øjemed, og tilsynet kan til brug for afgørelsen indhente oplysninger hos den pågældende, jf. persondatalovens § 62, stk. 1.

For så vidt angår denne vurdering, fremgår det endvidere af lovbemærkningerne, at det ikke er tilstrækkeligt, at den dataansvarlige selv er af den opfattelse, at der er tale om behandling, som finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed. Det understreges herefter i bemærkningerne til loven, at der påhviler den pågældende en vis forpligtelse til at sandsynliggøre, at vedkommendes aktiviteter falder ind under undtagelsesreglen.

Fra Datatilsynets praksis om lovens § 2, stk. 9, kan nævnes tilsynets udtalelse i sagen om Bastard Films produktion for Danmarks Radio (DR).[943] Sagen omhandlede en udsendelse, som Bastard Film havde lavet på baggrund af optagelser med skjult kamera på et bocenter for DR. Herefter klagede de ansatte på bocenteret til Datatilsynet bl.a. over, at Bastard Film ikke ville give oplysninger til de ansatte, om de havde yderligere optagelser af de pågældende end de, der blev vist i udsendelsen på DR, samt at de ansatte ikke kunne få lov til at se disse eventuelle yderligere optagelser. Datatilsynet fandt i denne sag, at Bastard Films behandling af personoplysninger for DR måtte anses for udelukkende at have et journalistisk øjemed, hvorfor behandlingen var omfattet af persondatalovens § 2, stk. 9.

[941] Datatilsynets j.nr. 2002-082-0075, gengivet i Persondataloven med kommentarer (2015), s. 124.
[942] Persondataloven med kommentarer (2015), s. 125.
[943] Datatilsynets j.nr. 2008-219-0133, gengivet i Persondataloven med kommentarer (2015), s. 125.

Herudover kan nævnes Datatilsynets udtalelse i sagen om lokal-tv fra overvågningskameraer i indkøbscenter i Voldsmose, som gengivet i tilsynets årsberetning 2006.[944] Sagen omhandlede et kunstnerisk og socialt projekt, hvor billeder fra overvågningskameraer i et indkøbscenter skulle transmitteres på storskærme i beboelsesområder.

Datatilsynets fandt i denne sag, at § 2, stk. 9, efter sin ordlyd ikke er indskrænket i forhold til lovens behandlingsbegreb, og at bestemmelsen derfor også kan anvendes på behandling, der i sig selv indebærer en offentliggørelse af personoplysninger.[945] I den konkrete sag fandt Datatilsynet, at det konkrete tv-projekt måtte anses at have et kunstnerisk såvel som et journalistisk øjemed, hvorfor den pågældende behandling af personoplysninger var det omfattet af lovens § 2, stk. 9. Dermed var det uden for Datatilsynets kompetence at tage stilling til projektets eventuelle behandling af personoplysninger.

Datatilsynets fandt i denne sag, at § 2, stk. 9, efter sin ordlyd ikke er indskrænket i forhold til lovens behandlingsbegreb, og at bestemmelsen derfor også kan anvendes på behandling, der i sig selv indebærer en offentliggørelse af personoplysninger.[946] I den konkrete sag fandt Datatilsynet, at det konkrete tv-projekt måtte anses at have et kunstnerisk såvel som et journalistisk øjemed, hvorfor den pågældende behandling af personoplysninger var det omfattet af lovens § 2, stk. 9. Dermed var det uden for Datatilsynets kompetence at tage stilling til projektets eventuelle behandling af personoplysninger. Projektet ville herefter alene være omfattet af bestemmelserne i lovens §§ 41, 42 og 69.[947]

10.1.3. Databeskyttelsesforordningen

10.1.3.1. Retten til beskyttelse af personoplysninger i forhold til andre grundlæggende rettigheder

Det fremgår af præambelbetragtning nr. 4, i databeskyttelsesforordningen, at retten til beskyttelse af personoplysninger ikke er en absolut ret, idet denne skal ses i sammenhæng med sin funktion i samfund og afvejes i forhold til andre grundlæggende rettigheder i Den Europæiske Unions charter for grundlæggende rettigheder i overensstemmelse med proportionalitetsprincippet.

Denne grundlæggende præmis for anvendelsen af EU-regler, herunder databeskyttelsesdirektivet og forordningen, må anses for at være en videreførelse af gældende ret, hvorefter de grundlæggende rettigheder, der følger af Den Europæiske Unions charter for grundlæg-

[944] Datatilsynets j.nr.2002-321-0155, ÅB, s. 42-44.
[945] Persondataloven med kommentarer (2015), s. 123.
[946] Persondataloven med kommentarer (2015), s. 123.
[947] Det skal bemærkes, at det fremgår af Lov om behandling af personoplysninger med kommentarer, at denne afgørelse muligvis går videre, end hvad der efter forarbejderne er lagt op til skulle være dens anvendelsesområde. Se også Peter Blume, Juristen nr. 1/2012.

gende rettigheder er værdisæt, som EU-Domstolene og medlemsstaterne iagttager ved fortolkningen af EU-regler.

Dernæst følger det af præambelbetragtning nr. 153, at forordningen overholder alle de grundlæggende rettigheder, og følger de frihedsrettigheder og principper, der anerkendes i chartret om grundlæggende rettigheder, som forankret i traktaten, navnlig retten til bl.a. informations- og ytringsfrihed.

I denne præambelbetragtning understreges det således – som i persondatalovens § 2, stk. 2 – at der ikke med forordningen gennemføres en regulering, der indebærer begrænsninger i de grundlæggende rettigheder, herunder retten til informations- og ytringsfrihed.

10.1.3.2. Rammerne for nationale særregler om behandling og ytrings- og informationsfrihed, artikel 85

Kommissionen anførte i forslaget fra 2012 til databeskyttelsesforordningen, at det oprindelige forslag til en bestemmelse om ytrings- og informationsfrihed var baseret på artikel 9, i databeskyttelsesdirektivet som fortolket af EU-Domstolen.[948] Det må således antages, at hensigten med bestemmelsen om ytrings- og informationsfrihed har været at videreføre den retstilstand, der følger af artikel 9 i direktivet.

Det fremgår af forordningens artikel 85, *stk. 1*, 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. Medlemsstaterne har således en forpligtelse til at foretage en afvejning af disse to hensyn og fastsætte nationale regler herom.

Ordet "herunder" viser, at anvendelsesområdet for artikel 85 ikke er begrænset til behandling i journalistisk øjemed og med henblik på akademisk, kunstnerisk eller litterær virksomhed.

For så vidt angår fortolkningen af begreberne journalistisk øjemed, akademisk, kunstnerisk eller litterær virksomhed, fremgår det af præambelbetragtning nr. 153, at det er nødvendigt at tolke begreber vedrørende ytringsfriheden, herunder f.eks. journalistik, bredt.

Dernæst fremgår det af forordningens artikel 85, *stk. 2*, at medlemsstaterne fastsætter undtagelser eller fravigelser fra visse dele af forordningen til behandling i journalistisk øjemed

[948] Kommissionens forslag af 25. januar 2012 (KOM(2012) 11 endelig), afsnit 3.4.9, s. 16.

eller med henblik på akademisk, kunstnerisk eller litterær virksomhed, hvis de er nødvendige for at forene retten til beskyttelse af personoplysninger med ytringsfrihed.

I modsætning til artikel 9 i direktivet, er akademisk litterær virksomhed nævnt direkte i forordningens artikel 85, *stk. 1* og *2*. Som anført ovenstående, følger det allerede af Datatilsynets praksis, at faglitterære bøger er omfattet af persondataloven, hvorfor der er tale om en videreførelse af den gældende retstilstand.

Det fremgår af forordningens præambelbetragtning nr. 153, at der bør fastsættes undtagelser eller fravigelser fra visse bestemmelser i forordning for behandling af personoplysninger, der udelukkende finder sted i journalistisk øjemed eller med henblik på akademisk, kunstnerisk eller litterær virksomhed, hvis det er nødvendigt for at forene retten til beskyttelse af personoplysninger med retten til ytrings- og informationsfrihed som garanteret ved artikel 11 i chartret om grundlæggende rettigheder.

Der kan i medfør af artikel 85, *stk. 2*, fastsættes undtagelser eller fravigelse fra forordningens kapitel II om principper, kapitel III om den registreredes rettigheder, kapitel IV om dataansvarlig og databehandler, kapitel V om overførsel af personoplysninger til tredjelande eller internationale organisationer, kapitel VI om uafhængige tilsynsmyndigheder, kapitel VII om samarbejde og sammenhæng og kapitel IX om specifikke behandlingssituationer.

Efter artikel 85, *stk. 2*, er det alene få kapitler i forordningen, som *ikke* kan undtages eller fraviges til behandling, der udelukkende sker i journalistisk øjemed eller med henblik på akademisk, kunstnerisk eller litterær virksomhed; forordningens kapitel I om de generelle bestemmelser, kapitel VIII om retsmidler, ansvar og sanktion og kapitel X om delegerede retsakter og gennemførelsesforanstaltninger.

Det skal hertil bemærkes, at de kapitler, der efter artikel 9 i direktivet kunne undtages og fraviges som følge af hensynet til ytrings- og informationsfriheden, indholdsmæssigt er lig de kapitler, der kan undtages i medfør af forordningens artikel 85, *stk. 2*. Forskellen består dog i, at forordningen indeholder en langt mere detaljeret regulering om de enkelte emner end direktivet.

I lighed med direktivets artikel 9 skal hver medlemsstat på baggrund af artikel 85, *stk. 2*, foretage en konkret afvejning af, hvilke fritagelser eller undtagelser fra reglerne i de angivne kapitler i forordningen, som anses for nødvendige for at forene retten til beskyttelse af personoplysninger med den grundlæggende ret til ytrings- og informationsfrihed.

Det må antages, at rammerne for at fastsætte nationale særregler, der undtager forordningens bestemmelser af hensyn til retten til informations- og ytringsfrihed svarer til det, der allerede følger af gældende ret efter direktivets artikel 9.

Der skal derfor i dansk ret foretages en afvejning af på den ene side hensynet til beskyttelse af personoplysninger, og på den anden side hensynet til informations- og ytringsfrihed med henblik på at sikre, at forordningens regler ikke unødigt medfører indskrænkninger i disse rettigheder.

For så vidt angår den eksisterende regel i persondatalovens § 2, stk. 4, hvorefter loven ikke finder anvendelse på behandling af oplysninger, der foretages for Folketinget og institutioner med tilknytning dertil, kan der med hjemmel i artikel 85 i en kommende udgave af persondataloven fastsættes nationale særregler.

Det må således antages, at der kan fastsættes nationale undtagelser og fravigelser fra de kapitler i forordningen, der er nævnt i artikel 85, stk. 2, af hensyn til informations- og ytringsfriheden i forbindelse med Folketingets parlamentariske arbejde. Når Folketingets Administration bistår Folketingets medlemmer i deres funktion som folketingsmedlemmer, må behandling i Folketingets Administration også antages at kunne undtages fra forordningen.

For så vidt angår de eksisterende regler i persondatalovens § 2, stk. 5-9, er disse også udtryk for en konkret afvejning i dansk ret af hensynet til beskyttelse af personoplysninger på den ene side og hensynet til informations- og ytringsfrihed på den anden side.[949]

Bestemmelserne i persondatalovens § 2, stk. 4-9, må herefter antages at kunne videreføres i det omfang, det vurderes, at disse undtagelser fortsat er nødvendige i dansk ret for at forene retten til beskyttelse af personoplysninger med den grundlæggende ret til informations- og ytringsfrihed.

For så vidt angår videreførelsen af reglerne i persondatalovens § 2, stk. 5-8, skal det endvidere bemærkes, at det fremgår af forordningens præambelbetragtning nr. 153, at undtagelser eller fravigelser fra visse bestemmelser i forordningen, navnlig bør gælde for behandling af personoplysninger på det audiovisuelle område og i nyhedsarkiver og pressebiblioteker.

[949] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 208.

Det skal endvidere bemærkes, at det må antages, at forordningens artikel 85, stk. 2, kan medføre varierende fravigelser eller undtagelser fra én medlemsstat til en anden. Hertil bemærkes det i forordningens præambelbetragtning nr. 153, at den nationale ret i den medlemsstat, som den dataansvarlige er underlagt, finder anvendelse.

For så vidt angår retten til at blive glemt skal det bemærkes, at denne rettighed ikke finder anvendelse, i det omfang en behandling af personoplysninger er nødvendig for at udøve retten til ytrings- og informationsfrihed, jf. forordningens artikel 17, stk. 3, litra a.

Endelig fremgår det af artikel 85, *stk. 3*, at hver medlemsstat giver Kommissionen meddelelse om de regler, som den vedtager i henhold til *stk. 2*, og underretter den straks om alle senere ændringer, der berører dem.

10.1.4. Overvejelser

Databeskyttelsesforordningens artikel 85 ses ikke at udgøre en ændring af gældende ret, hvorefter retten til beskyttelse af personoplysninger skal ses i sammenhæng med og afvejes i forhold til andre grundlæggende rettigheder i overensstemmelse med proportionalitetsprincippet.

Dermed må det antages, at gældende ret efter persondatalovens § 2, stk. 2, kan videreføres efter den 25. maj 2018, hvorfra forordningen skal anvendes.

Efter artikel 85, *stk. 1* og *stk. 2*, er medlemsstaterne endvidere forpligtede til at foretage en afvejning af hensynet til beskyttelse af personoplysninger og retten til informations- og ytringsfrihed samt til at fastsætte nationale regler herom.

Medlemsstaternes mulighed for at fastsætte undtagelser og fravigelser fra visse af forordningens bestemmelser af hensyn til retten til informations- og ytringsfrihed vil overordnet ikke være en ændring i forhold til gældende ret.

Det må således antages, at persondatalovens § 2, stk. 5-9, vil kunne videreføres i det omfang, det vurderes, at disse undtagelser fortsat er nødvendige i dansk ret for at forene retten til beskyttelse af personoplysninger med den grundlæggende ret til informations- og ytringsfrihed. På samme måde vil det – af hensyn til informations- og ytringsfriheden – være muligt at fastsætte undtagelser og fravigelser fra forordningen, for så vidt angår Folketingets medlemmers behandling af personoplysninger.

10.2. Rammerne i artikel 86 om behandling og aktindsigt i officielle dokumenter mv.

10.2.1. Præsentation

Artikel 86 fastslår, at personoplysninger i officielle dokumenter, som en offentlig myndighed eller et offentligt eller privat organ er i besiddelse af med henblik på udførelse af en opgave i samfundets interesse, må *videregives* af myndigheden eller organet *i overensstemmelse med EU-retten* eller *medlemsstaternes nationale ret*, som den offentlige myndighed eller organet er underlagt, for at forene *aktindsigt* i officielle dokumenter med retten til beskyttelse af personoplysninger i henhold til forordningen.

Det fremgår desuden af præambelbetragtning nr. 154, at personoplysninger i dokumenter, der opbevares af en offentlig myndighed eller et offentligt organ, bør kunne *offentliggøres* af denne myndighed eller dette organ, hvis dette er fastsat i EU-retten eller i medlemsstaternes nationale ret, som den offentlige myndighed eller det offentlige organ er underlagt.

For så vidt angår aktindsigt i personoplysninger, som vedrører behandlinger omfattet af forordningens artikel 2, stk. 2, litra d, om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger (retshåndhævelsesdirektivet), bemærkes for en god ordens skyld, at spørgsmål om aktindsigt i denne sammenhæng ikke er omfattet af forordningens materielle anvendelsesområde.

10.2.2. Gældende ret

10.2.2.1. Forholdet til offentlighedsloven og forvaltningsloven

I dansk ret regulerer offentlighedsloven den almindelige adgang for offentligheden til efter begæring at få aktindsigt i forvaltningsmyndighedernes dokumenter. Efter offentlighedsloven tilkommer retten til aktindsigt enhver, ligesom retten som udgangspunkt omfatter alle typer af dokumenter og oplysninger. Ved siden af offentlighedslovens almindelige regler om aktindsigt er der også fastsat nogle mere specifikke regler om indsigt mv. i forvaltningsloven, sundhedsloven, miljøoplysningsloven, arkivloven og retsplejeloven.

Om samspillet mellem reglerne om indsigt efter persondataloven, forvaltningsloven og offentlighedsloven fremgår det af lovforslaget, der førte til persondataloven[950], at spørgs-

[950] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.11.3. i de almindelige bemærkninger.

målet om *tredjemands ret til aktindsigt i oplysninger om andre personer* skal afgøres efter anden lovgivning end persondataloven, herunder offentlighedsloven.

Om forholdet mellem persondataloven og *offentlighedsloven* fremgår det i forlængelse heraf af persondataloven med kommentarer[951], at der i lyset af persondatalovens klare forarbejder på dette punkt ikke er grundlag for en antagelse om, at forvaltningsmyndigheder (tillige) skal have hjemmel i behandlingsreglerne i persondataloven, f.eks. § 5 og §§ 6-8, til at foretage de nødvendige skridt til opfyldelse af en pligt efter offentlighedsloven til at give aktindsigt.

Der er både ret til egenacces efter persondataloven og ret til aktindsigt (egenacces) efter reglerne i offentlighedsloven. Afgørelsen skal træffes på det retsgrundlag, der er mest gunstigt for den pågældende.

Offentlighedslovens § 11 indeholder en bestemmelse om, at enhver under visse betingelser kan forlange, at en forvaltningsmyndighed foretager og udleverer en sammenstilling af foreliggende oplysninger i myndighedens databaser (dataudtræk).

Som nævnt fastslår offentlighedsloven, at enhver som udgangspunkt har ret til aktindsigt i forvaltningsmyndighedernes dokumenter. Loven indeholder imidlertid en række modifikationer til dette udgangspunkt. Der er således i offentlighedslovens kapitel 4 fastsat nærmere regler om, at loven ikke gælder visse sagstyper, visse dokumenttyper og visse oplysningstyper, ligesom retten til aktindsigt er begrænset af særlige bestemmelser om tavshedspligt.

Om forholdet mellem persondataloven og offentlighedsloven fremgår det desuden af persondataloven med kommentarer[952], at persondatalovens behandlingsregler (det vil i praksis sige §§ 6-8) alene, har betydning i relation til spørgsmålet om adgang til at give *meroffentlighed* i personoplysninger.

Offentlighedslovens § 14 indeholder således en bestemmelse om meroffentlighed, hvorefter det i forbindelse med en anmodning om aktindsigt *skal* overvejes, om der kan gives aktindsigt i dokumenter og oplysninger i videre omfang, end hvad der følger af bestemmelserne om undtagelser til retten til aktindsigt, samt at der kan gives aktindsigt i videre omfang, medmindre det vil være i strid med anden lovgivning, herunder regler om tavshedspligt og regler i lov om behandling af personoplysninger.

[951] Persondataloven med kommentarer (2015), s. 693.
[952] Persondataloven med kommentarer (2015), s. 693 og s. 695 f.

Om forholdet mellem persondataloven og *forvaltningsloven* fremgår det af persondataloven med kommentarer[953], at der kun er sammenfald mellem forvaltningslovens partsaktindsigtsregler og persondatalovens indsigtsregler for så vidt angår retten til at få oplysninger om sig selv.

Det fremgår desuden af persondataloven med kommentarer[954], at aktindsigtsreglerne i forvaltningsloven regulerer spørgsmålet om parters adgang til aktindsigt i afgørelsessager, medens persondataloven regulerer spørgsmålet om egenacces. Retten for den, der er part i en sag, til at få partsaktindsigt efter forvaltningslovens regler *i personoplysninger, som fremgår af sagsakterne vedrørende andre personer* er således ikke berørt af persondataloven, og den består dermed fortsat. Det gælder selv følsomme oplysninger, med den begrænsning, der ligger i forvaltningslovens regler om undtagelse af oplysninger fra partens ret til aktindsigt.[955]

Forvaltningslovens § 10 indeholder i øvrigt en bestemmelse om *meroffentlighed*, som svarer til bestemmelsen om meroffentlighed i offentlighedslovens § 14.

10.2.2.2. Videreanvendelse

Om *videreanvendelse* af personoplysninger, som er udleveret i henhold til offentlighedslovens regler om aktindsigt, f.eks. oplysninger om offentligt ansattes løn, fremgår det af persondataloven med kommentarer[956], at dette spørgsmål må afgøres ud fra persondatalovens regler om behandling, herunder videregivelse af personoplysninger – naturligvis forudsat, at den pågældende videre anvendelse af oplysningerne er omfattet af persondatalovens anvendelsesområde.

Det følger af *lov om videreanvendelse af den offentlige sektors informationer*[957] § 4, stk. 1, at offentlige myndigheder, herunder biblioteker, museer og arkiver, kan stille dokumenter og datasamlinger til rådighed for videreanvendelse, medmindre lovens øvrige bestemmelser eller anden lovgivning er til hinder herfor. Det fremgår af forarbejderne til bestemmelsen[958], at dette bl.a. ikke ændrer på gældende regler om adgang til aktindsigt efter offentlighedsloven og forvaltningsloven eller reglerne i persondataloven.

[953] Persondataloven med kommentarer (2015), s. 691.
[954] Persondataloven med kommentarer (2015), s. 691.
[955] Persondataloven med kommentarer (2015), s. 691.
[956] Persondataloven med kommentarer (2015), s. 693 f.
[957] Lov nr. 596 af 24. juni 2005 med senere ændringer.
[958] Forslag nr. 156 af 14. marts 2014, FT 2013/14, om ændring af lov om videreanvendelse af den offentlige sektors informationer, de almindelige bemærkninger pkt. 3.5.2.

Loven gennemfører dele af *Europa-Parlamentets og Rådets direktiv 2003/98/EF* af 17. november 2003 om videreanvendelse af den offentlige sektors informationer.

10.2.2.3. Postlister

Det fremgår af Betænkning om offentlighedsloven[959], at en række myndigheder i forbindelse med etablering af hjemmesider på internettet også har etableret såkaldte åbne *postlister* på internettet, dvs. offentlige fortegnelser, der indeholder oplysninger om de dokumenter, som den pågældende myndighed enten har modtaget eller afsendt i en vis periode, uden at der har været fastsat nærmere regler om postlister, herunder regler, der forpligter forvaltningsmyndighederne til at føre sådanne lister.[960]

Det fremgår desuden af Betænkning om offentlighedsloven[961], at der, i det omfang en forvaltningsmyndighed vælger at føre en postliste, der ikke er offentligt tilgængelig, vil være adgang til aktindsigt i listen efter offentlighedslovens almindelige regler.

Om postlister fremgår det af persondataloven med kommentarer[962], at offentlige myndigheder på en hjemmeside eller på anden måde kan *offentliggøre* postlister. Sådanne postlister vil normalt indeholde (kortfattede) oplysninger såsom journalnummer, sagsnavn, brevdato eller registreringsdato, partens eller parternes navne, kort omtale af brevets indhold og angivelse af den ansvarlige afdeling. Det er dog et krav, at der ikke videregives fortrolige oplysninger. En postliste må derfor kun indeholde sådanne oplysninger, som der ville kunne gives aktindsigt i efter reglerne i offentlighedsloven, eventuelt i form af meroffentlighed.[963]

Det fremgår i øvrigt af offentlighedslovens § 16, at der for nærmere angivne myndigheder ved bekendtgørelse kan etableres ordninger med *pligtmæssige postlister*, som skal offentliggøres på myndighedens hjemmeside. Om indholdet af pligtmæssige postlister fremgår det nærmere af offentlighedslovens § 16, stk. 2, 2. pkt., at postlisten skal indeholde oplysninger om 1) dato for dokumentets modtagelse eller afsendelse, 2) navnet på eller eller karakteren af modtageren eller afsenderen af dokumentet, 3) kort tematisk angivelse af dokumentets indhold, og 4) journalnummer eller anden identifikationsbetegnelse. Det fremgår af bemærkningerne til lovforslaget, der førte til offentlighedsloven[964], at det er

[959] Betænkning nr. 1510/2009 om offentlighedsloven, bind 2, s 815.
[960] Betænkning nr. 1510/2009 om offentlighedsloven, bind 2, s 815 f.
[961] Betænkning nr. 1510/2009 om offentlighedsloven, bind 2, s 816.
[962] Persondataloven med kommentarer (2015), s. 244.
[963] Persondataloven med kommentarer (2015), s. 244.
[964] Forslag nr. 144 til lov om offentlighed i forvaltningen fremsat 7. februar 2013, FT 2012/13, de specielle bemærkninger til § 16.

forudsat, at postlisten bl.a. ikke indeholder fortrolige oplysninger, der er omfattet af persondatalovens §§ 6-8.

10.2.3. Databeskyttelsesforordningen

10.2.3.1.1. Det fremgår af artikel 86, at personoplysninger i officielle dokumenter, som en offentlig myndighed eller et offentligt eller privat organ er i besiddelse af med henblik på udførelse af en opgave i samfundets interesse, må videregives af myndigheden eller organet i overensstemmelse med EU-retten eller medlemsstaternes nationale ret, som den offentlige myndighed eller organet er underlagt, for at forene aktindsigt i officielle dokumenter med retten til beskyttelse af personoplysninger i henhold til forordningen.

Det fremgår af præambelbetragtning nr. 154, at forordningen giver mulighed for, at der ved anvendelsen af forordningen kan tages hensyn til princippet om aktindsigt i officielle dokumenter, og at aktindsigt i officielle dokumenter kan anses for at være i samfundets interesse.

Det fremgår desuden af præambelbetragtning nr. 154, at personoplysninger i dokumenter, der opbevares af en offentlig myndighed eller et offentligt organ, bør kunne offentliggøres af denne myndighed eller dette organ, hvis dette er fastsat i EU-retten eller i medlemsstaternes nationale ret, som den offentlige myndighed eller det offentlige organ er underlagt. Sådanne regler bør forene aktindsigt i officielle dokumenter og videreanvendelse af den offentlige sektors information med retten til beskyttelse af personoplysninger i henhold til forordningen, og kan derfor indeholde den nødvendige forening med retten til beskyttelse af personoplysninger i henhold til denne forordning.

10.2.3.1.2. I lyset af ordlyden i artikel 86, hvorefter bl.a. personoplysninger i officielle dokumenter må *videregives i overensstemmelse med EU-retten eller medlemsstaternes nationale ret* for at *forene* aktindsigt i officielle dokumenter med retten til beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen, må det antages, at spørgsmål om aktindsigt *ikke* skal vurderes efter databeskyttelsesforordningen, men i overensstemmelse med EU-retten eller medlemsstaternes nationale ret, i det omfang EU-retten eller medlemsstaternes nationale ret er fastsat bestemmelser, som *forener* retten til aktindsigt i officielle dokumenter med retten til beskyttelse af personoplysninger i henhold til denne forordning.

10.2.3.2. Det fremgår af præambelbetragtning nr. 154, at Europa-Parlamentets og Rådets direktiv 2003/98/EF opretholder og på ingen måde griber ind i beskyttelsesniveauet for fysiske personer med hensyn til behandling af personoplysninger i henhold til EU-retten og medlemsstaternes nationale ret, og navnlig ikke ændrer de forpligtelser og rettigheder, der er fastsat i forordningen.

Dette svarer til indholdet af artikel 1, stk. 4, i direktiv 2003/98/EF om videreanvendelse af den offentlige sektors informationer, hvor der dog henvises til databeskyttelsesdirektivet, i stedet for forordningen.

Det fremgår desuden af præambelbetragtning nr. 154, at direktivet om videreanvendelse af den offentlige sektors informationer navnlig ikke bør gælde for dokumenter, hvortil adgang er udelukket eller begrænset i henhold til aktindsigtsordninger under henvisning til beskyttelse af personoplysninger, og dele af dokumenter, der i henhold til disse ordninger er adgang til, og som indeholder personoplysninger, hvis videreanvendelse ifølge lovgivningen er uforenelig med lovgivningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

Dette svarer til indholdet af artikel 1, stk. 2, litra cc, i direktivet om videreanvendelse af den offentlige sektors informationer.[965]

Samlet set må det derfor lægges til grund, at denne del af præambelbetragtning nr. 154 skal forstås som en videreførelse af gældende ret i relation til direktivet om videreanvendelse af den offentlige sektors informationer.

10.2.3.3. Det slås i øvrigt i præambelbetragtning nr. 154 fast, at offentlige myndigheder og organer i relation til princippet om aktindsigt bør omfatte alle myndigheder eller andre organer, der er omfattet af medlemsstaternes nationale ret om aktindsigt.

10.2.4. Overvejelser

Spørgsmål om aktindsigt skal ikke afgøres på grundlag af forordningen i det omfang, der i EU-retten eller national ret er fastsat regler, som forener aktindsigt i officielle dokumenter med retten til beskyttelse af personoplysninger.

Offentlighedsloven indeholder en række undtagelser til hovedreglen om, at enhver som udgangspunkt har ret til aktindsigt i forvaltningsmyndighedernes dokumenter. Loven gælder således ikke for visse sagstyper, visse dokumenttyper og visse oplysningstyper, ligesom retten til aktindsigt er begrænset af særlige bestemmelser om tavshedspligt.

Som det er anført ovenfor om gældende ret, fremgår det direkte af offentlighedslovens § 14, at der kan gives meroffentlighed, *medmindre* det vil være i strid med anden lovgivning, herunder regler om tavshedspligt og regler i lov om behandling af personoplysninger.

[965] Europa-Parlamentets og Rådets direktiv 2013/37/EU af 26. juni 2013 om ændring af direktiv 2003/18/EF om videreanvendelse af den offentlige sektors informationer.

Denne retstilstand må antages at kunne opfylde betingelsen i forordningens artikel 86, hvorefter retten til aktindsigt skal *forenes* med retten til beskyttelse af personoplysninger, og det kan derfor lægges til grund, at retten til *aktindsigt for enhver* således også efter 25. maj 2018 vil skulle vurderes på grundlag af reglerne i offentlighedsloven, herunder om der skal gives meroffentlighed i overensstemmelse med offentlighedslovens § 14, og at forordningen – som det hidtil har gjort sig gældende i relation til persondataloven – vil skulle iagttages i forbindelse med spørgsmål om meroffentlighed.

Tilsvarende gør sig gældende for så vidt angår spørgsmål om aktindsigt i medfør af de specifikke regler om *parters adgang til aktindsigt* i medfør af forvaltningsloven. I relation til de regler, som skal forene aktindsigt og beskyttelse af personoplysninger i denne sammenhæng, må det tages i betragtning, at formålet med reglerne om parters adgang til aktindsigt bl.a. er at give en part i en sag lejlighed til at gøre sig bekendt med sagens dokumenter og oplysninger og på den baggrund tage stilling til, om de oplysninger, der indgår i sagen, bør suppleres eller korrigeres. Hertil kommer et bredere princip i dansk forvaltningsret, hvorefter en part – uanset om formålet med aktindsigt er at påvirke en myndigheds beslutningsproces i sagen – har ret til at se alle sagens oplysninger og dokumenter. Undtagelse fra dette grundlæggende princip kræver tungtvejende grunde.[966]

Ligeledes gør sig gældende for specifikke regler om aktindsigt i anden lovgivning, f.eks. miljøoplysningsloven, dvs. specifikke spørgsmål om aktindsigt i dokumenter omfattet af disse regelsæt skal også efter 25. maj 2018 afgøres på grundlag af disse regler og ikke forordningens bestemmelser, i det omfang, der i disse specifikke regelsæt er fastsat regler, som forener retten til aktindsigt med retten til beskyttelse af personoplysninger.

Som anført ovenfor har en række myndigheder i forbindelse med etablering af hjemmesider etableret (frivillige) postlister på internettet, uden at der har været fastsat nærmere regler herom. I det omfang, der ikke er fastsat nærmere regler om myndighedernes offentliggørelse af postlister, må det i lyset af præambelbetragtning nr. 154 antages, at disse offentliggørelser fra 25. maj 2018 skal ske under iagttagelse af databeskyttelsesforordningen.

Som anført ovenfor giver offentlighedsloven mulighed for ved bekendtgørelse at etablere ordninger med pligtmæssige postlister, og det er i den i forbindelse forudsat, at postlisten ikke indeholder fortrolige oplysninger, der er omfattet af persondatalovens §§ 6-8. Ordninger med pligtmæssige bekendtgørelser af postlister etableret i medfør af offentlighedslovens § 16 må antages at opfylde betingelserne i præambelbetragtning nr. 154, hvorefter offentlige myndigheder bl.a. kan offentliggøre personoplysninger i dokumenter, hvis dette

[966] Niels Fenger, Forvaltningsloven med kommentarer, 1. udgave (2013), s. 314-315.

er *fastsat i medlemsstaternes nationale ret*, idet sådanne regler bør forene aktindsigt og beskyttelse af personoplysninger. Ordninger med pligtmæssige postlister vil således fra maj 2018 skulle vurderes på grundlag af de regler, som udstedes i medfør af offentlighedslovens § 16.

10.3. Rammerne i artikel 87 vedrørende nationalt identifikationsnummer

10.3.1. Præsentation

Persondatalovens § 11 vedrører, i hvilket omfang offentlige myndigheder og private kan behandle oplysninger om personnummer. Bestemmelsen er baseret på artikel 8, stk. 7, i databeskyttelsesdirektivet, hvorefter medlemsstaterne kan bestemme, på hvilke betingelser et nationalt identifikationsnummer kan gøres til genstand for behandling.

Databeskyttelsesforordningen indeholder en tilsvarende bestemmelse i artikel 87, hvorefter medlemsstaterne har mulighed for at fastsætte specifikke betingelser for behandling af et nationalt identifikationsnummer.

10.3.2. Gældende ret

Det følger af artikel 8, stk. 7, i databeskyttelsesdirektivet, at medlemsstaterne bestemmer, på hvilke betingelser et nationalt identifikationsnummer eller andre almene midler til identifikation kan gøres til genstand for behandling.

Registerudvalget anførte i betænkning nr. 1345, at medlemsstaterne – og dermed også udvalget – på baggrund af direktivets artikel 8, stk. 7, er frit stillet med hensyn til spørgsmålet om, hvilke regler der bør gælde for behandling af oplysninger om personnummer.[967]

Der er på denne baggrund fastsat nationale særregler i persondatalovens § 11 for, i hvilket omfang offentlige myndigheder og private kan behandle oplysninger om personnummer.

10.3.2.1. Offentlige myndigheders behandling af personnummer

Det fremgår af persondatalovens § 11, stk. 1, at offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer.

Det fremgår af bemærkningerne til persondataloven, at bestemmelsen ikke indebærer, at en forvaltningsmyndighed må føre åbne postlister, hvor borgernes personnumre er anvendt som journalnummer.[968]

[967] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 259-260.

Det følger af Datatilsynets udtalelse i en sag om Holbæk Kommunes videregivelse af personnumre til TDC A/S,[969] at en offentlig myndighed kun må videregive personnumre til en privat dataansvarlig, hvis den private dataansvarlige har hjemmel til at behandle disse oplysninger.

Herudover skal offentlige myndigheder iagttage regler om behandling af personnummer i CPR-loven.

10.3.2.2. Privates behandling af personnummer

Det fremgår af persondatalovens § 11, stk. 2, at private kan behandle oplysninger om personnummer efter de i nr. 1-3, angivne tilfælde.

Det fremgår af persondatalovens § 11, stk. 2, *nr. 1*, at private må behandle oplysninger om personnummer, når det følger af lov eller bestemmelser fastsat i henhold til lov. Som eksempel herpå kan nævnes privates oplysningsforpligtelse over for SKAT for så vidt angår indberetning af forskellige indkomstrelaterede oplysninger i medfør af skattelovgivningen.[970]

Herudover skal private i visse tilfælde iagttage regler om behandling af personnummer i CPR-loven.[971]

Det følger endvidere af Datatilsynets praksis,[972] at hvis en privat dataansvarlig kan behandle oplysninger om personnummer på baggrund af en særlig hjemmel i lovgivningen, kan den dataansvarlige også anvende oplysningerne internt til administrative formål, der har en sammenhæng med den behandling, som der er særlig hjemmel til.

Dernæst fremgår det af persondatalovens § 11, stk. 2, *nr. 2*, at der vil kunne ske behandling af personnummer, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Samtykket skal efterleve betingelserne i persondatalovens § 3, nr. 8.

Det fremgår af persondatalovens § 11, stk. 2, *nr. 3, 1. led,* at private i visse tilfælde kan behandle oplysninger om personnummer uden samtykke, nemlig hvis behandlingen af personnumre alene sker i forbindelse med undersøgelser i videnskabeligt eller statistisk øjemed.

---

[968] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 11.
[969] Datatilsynets j.nr. 2007-313-0056.
[970] Persondataloven med kommentarer (2015), s. 335.
[971] Persondataloven med kommentarer (2015), s. 334.
[972] Se f.eks. Datatilsynets j.nr. 2000-214-0005.

Herudover kan der på baggrund af persondatalovens § 11, stk. 2, *nr. 3, 2. led*, ske videregivelse af oplysninger om personnummer, når videregivelsen er et naturligt led i den normale drift af virksomheder mv. af den pågældende art, og når videregivelsen er af afgørende betydning for at sikre en entydig identifikation af den registrerede eller videregivelsen kræves af en offentlig myndighed.

Det fremgår af bemærkningerne til persondataloven, at bestemmelsen indebærer, at registrerede oplysninger om personnumre kan videregives i samme omfang som efter den hidtil gældende retstilstand i registerlovgivningen. [973] Der er således mulighed for at opretholde den hidtidige adgang til – på grundlag af kundernes personnumre – at foretage samkøring i den finansielle sektor.

Endelig fremgår det af persondatalovens § 11, *stk. 3*, at uanset bestemmelsen i stk. 2, nr. 3, må der ikke ske offentliggørelse af personnummer uden udtrykkeligt samtykke.

10.3.3. Databeskyttelsesforordningen

Det fremgår af forordningens artikel 87, *1. pkt.*, at medlemsstaterne nærmere *kan* fastsætte de specifikke betingelser for behandling af et nationalt identifikationsnummer eller andre almene midler til identifikation.

For så vidt angår forholdet mellem forordningens artikel 87, 1. pkt., og databeskyttelsesdirektivets artikel 8, stk. 7, 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 om, at *medlemsstaterne bestemmer, på hvilke betingelser* behandling af personnummer kan ske, hvor der i forordningen tales om, at *medlemsstaterne kan nærmere fastsætte de specifikke betingelser* for behandling af personnummer.

De sproglige forskelle ses dog ikke at have en indholdsmæssig betydning i forhold til gældende ret, idet medlemsstaterne fortsat i medfør af forordningens artikel 87 kan fastsætte nationale særregler om behandling af oplysninger om identifikationsnummer eller andre midler til identifikation.

Det følger endvidere af forordningens artikel 87, *2. pkt.*, at det nationale identifikationsnummer eller ethvert andet alment middel til identifikation udelukkende anvendes med de

[973] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 11.

fornødne garantier for den registreredes rettigheder og frihedsrettigheder i henhold til forordningen.

Forordningens artikel 87, 2. pkt. må antages at betyde, at der i de nationale særregler om behandling af identifikationsnummer mv., skal tages hensyn til behovet for databeskyttelse, så disse oplysninger udelukkende anvendes med de fornødne garantier for den registreredes rettigheder og frihedsrettigheder i henhold til forordningen.

Som anført ovenfor er der i dansk ret fastsat særlige regler for, hvornår offentlige myndigheder og private må behandle oplysninger om personnummer, hvilket har til formål at sikre, at disse oplysninger alene kan behandles, såfremt nærmere bestemte og specifikke betingelserne i loven er opfyldt.

Persondatalovens § 11 må antages at medføre, at oplysninger om personnummer udelukkende anvendes med de "fornødne garantier" for den registreredes rettigheder og frihedsrettigheder i den forstand udtrykket anvendes i artikel 87, 2. pkt. For eksempel indeholder persondatalovens § 11, stk. 3, således som nævnt den begrænsning, at private ikke må offentliggøre oplysninger om personnummer uden udtrykkeligt samtykke. På baggrund heraf må det antages, at persondatalovens § 11 kan videreføres inden for rammerne af forordningens artikel 87.

10.3.4. Overvejelser

Databeskyttelsesforordningens artikel 87 må anses for at være udtryk for en videreførelse af gældende ret, dog med den tilføjelse, at behandling af oplysninger om identifikationsnummer mv. udelukkende anvendes med de fornødne garantier for den registreredes rettigheder og frihedsrettigheder i henhold til forordningen.

Persondatalovens § 11 vurderes at respektere forordningens krav i artikel 87 om, at oplysninger om personnummer udelukkende anvendes med de fornødne garantier for den registreredes rettigheder og frihedsrettigheder i henhold til forordningen, hvorfor bestemmelsen må antages at kunne videreføres inden for rammerne af forordningens artikel 87.

10.4. Rammerne i artikel 88 vedrørende behandling i forbindelse med ansættelsesforhold

10.4.1. Præsentation

Forordningens artikel 88 angiver – som noget nyt – en mulighed for at fastsætte nationale supplerende særregler om behandling af arbejdstageres personoplysninger i forbindelse med ansættelsesforhold.

I medfør af artikel 88, stk. 1, kan medlemsstaterne ved *lov* eller i medfør af *kollektive overenskomster* fastsætte mere specifikke bestemmelser for at sikre beskyttelse af rettighederne og frihedsrettighederne i forbindelse med behandling af *arbejdstagernes personoplysninger i ansættelsesforhold*, navnlig med henblik på ansættelse, ansættelseskontrakter, herunder opfyldelse af forpligtelser fastsat ved lov eller i kollektive overenskomster, ledelse, planlægning og tilrettelæggelse af arbejdet, ligestilling og mangfoldighed på arbejdspladsen, arbejdsmiljø samt beskyttelse af arbejdsgiveres eller kunders ejendom og med henblik på individuel eller kollektiv udøvelse og nydelse af rettigheder og fordele i forbindelse med ansættelse samt med henblik på ophør af ansættelsesforhold.

Det fremgår af artikel 88, stk. 2, at disse bestemmelser skal omfatte *passende og specifikke foranstaltninger* til beskyttelse af den registreredes menneskelige værdighed, legitime interesser og grundlæggende rettigheder, særlig med hensyn til gennemsigtighed i behandlingen, overførsel af personoplysninger inden for en koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet, og overvågningssystemer på arbejdspladsen.

Det fremgår af artikel 88, stk. 3, at hver medlemsstat senest den 25. maj 2018 giver *Kommissionen meddelelse* om de lovbestemmelser, som den vedtager i henhold til stk. 1, og *underretter* den straks om alle senere ændringer, der berører dem.

10.4.2. Gældende ret

Persondataloven fastlægger en generel ramme for behandling af arbejdstagernes personoplysninger i forbindelse med ansættelsesforhold.

Ansættelsesforhold er desuden på en række områder specifikt reguleret i anden lovgivning, f.eks. vedrørende arbejdsmiljø, jobformidling og arbejdsløshedsforsikring, mens regulering af løn- og arbejdsvilkår sker gennem kollektive overenskomster.

Der har på en række områder udviklet sig en særlig praksis for behandling af personoplysninger i forbindelse med ansættelsesforhold, hvor de arbejdsretlige regler og kollektive

overenskomster mv. er af betydning for udfyldningen af de generelle regler i persondataloven. Særligt for så vidt angår behandling af oplysninger på grundlag af samtykke fremgår det af Persondataret i ansættelsesforhold, at en fagforenings, en tillidsrepræsentants eller et samarbejdsudvalgs (arbejdsretlige) samtykke til en specifik kontrolforanstaltning ikke i sig selv vil kunne udgøre det fornødne behandlingsgrundlag efter §§ 6-8. Et kollektivt samtykke udgør dermed heller ikke i denne sammenhæng et gyldigt samtykke, men vil i sagens natur kunne indgå som et element i den interesseafvejning, der skal foretages efter f.eks. § 6, stk. 1, nr. 7. [974]

I det følgende vil de generelle regler i persondataloven blive gennemgået, og herefter berøres en række af de specifikke behandlingssituationer, hvor der har udviklet sig en særlig praksis. Endelig vil gældende ret vedrørende ansættelsesforhold i form af særlovgivningen og kollektive overenskomster blive omtalt.

10.4.2.1. Persondataloven

Af særlig relevans i forbindelse med arbejdsforhold er bestemmelsen i persondatalovens § 6, stk. 1, nr. 2, hvorefter behandling af oplysninger må finde sted, hvis behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den registrerede er part i, eller hvis behandlingen er nødvendig af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en aftale. Aftaler om ansættelse er således omfattet af lovens § 6, stk. 1, nr. 2.

For så vidt angår behandlinger, der sker i henhold til kollektive overenskomster, har navnlig persondatalovens § 6, stk. 1, nr. 7, vist sig at være relevant som behandlingsgrundlag og efter omstændighederne også lovens 6, stk. 1, nr. 3, hvis behandlingen i det kollektivretlige system hviler på lovgivning.

Desuden vil bestemmelsen i persondatalovens § 7, stk. 3, hvorefter behandling af oplysninger om fagforeningsmæssige tilhørsforhold kan ske, hvis behandlingen er nødvendig for overholdelsen af den dataansvarliges arbejdsretlige forpligtelser eller specifikke rettigheder, antages at være relevant i praksis i forbindelse med ansættelsesforhold. Det fremgår af bemærkningerne til lovforslaget, der førte til persondataloven[975], 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

[974] Peter Blume og Jens Kristiansen, Persondataret i ansættelsesforhold, 1. udgave, 2011, s. 66.
[975] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7, stk. 3.

overenskomster mellem arbejdsmarkedets parter eller af individuelle ansættelseskontrakter, er dermed omfattet af bestemmelsen. Det bemærkes, at den behandling som finder sted – som ved al behandling af personoplysninger – naturligvis ikke må gå ud over rammerne for de grundlæggende principper for behandling af oplysninger, jf. § 5[976].

Jens Kristiansen og Peter Blume anfører, at arbejdsgiveren i henhold til § 7, stk. 3, kan og skal videregive oplysninger i alle de tilfælde, hvor der er en overenskomstmæssig funderet pligt til at udlevere oplysninger. Det følger af persondatalovens § 7, stk. 3, at dataansvarlige generelt er berettigede til at behandle oplysninger, herunder videregive oplysninger, om "fagforeningsmæssigt tilhørsforhold" (som er en følsom oplysning), hvis det er nødvendigt for at overholde en arbejdsretlig forpligtelse. En tilsvarende bestemmelse som persondatalovens § 7, stk. 3, er ikke nævnt blandt de opregnede behandlingsgrundlag i § 6, men forfatterne antager det som nærliggende, at den må have afsmittende virkninger her. Arbejdsgiverens interesse i at kunne overholde sine overenskomstmæssige forpligtelser må som altovervejende hovedregel veje tungere, end den enkelte lønmodtagers interesse i at undgå videregivelse. [977]

For så vidt angår samtlige de i § 7, stk. 1, nævnte følsomme oplysninger, bemærkes det desuden, at den dataansvarlige adgang til at foretage behandling af oplysninger med henblik på at overholde dennes arbejdsretlige forpligtelser eller udøve dennes specifikke arbejdsretlige rettigheder må antages at være begrænset til oplysninger om enkeltpersoners fagforeningsmæssige forhold.[978]

For så vidt angår arbejdsgiveres behandling af oplysninger om *strafbare forhold*, f.eks. i en straffeattest, er dette reguleret i persondatalovens § 8, stk. 1, 4 og 6, jf. § 5, alt efter, om der er tale om offentlige eller private arbejdsgivere, samt yderligere reguleret i kriminalregisterbekendtgørelsen[979]. Der henvises til afsnit 3.10 og 3.11. om forordningens artikel 10.

10.4.2.1.1. Nærmere om behandling af ikke-følsomme oplysninger i forbindelse med personaleadministration

Det fremgår af lov om behandling af personoplysninger med kommentarer[980], at en arbejdsgiver – privat eller offentlig – i et personaleregister vil 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 per-

[976] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 7, stk. 3.
[977] Peter Blume og Jens Kristiansen: Persondataret i ansættelsesforhold, 1. udgave, 2011, s. 117.
[978] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 238.
[979] Bekendtgørelsen nr. 881 af 4. juli 2014 med senere ændringer.
[980] Persondataloven med kommentarer (2015), s 219.

sondatalovens § 6, stk. 1, nr. 2. Der kan være tale om forskellige stamoplysninger, som f.eks. navn, adresse, personnummer, oplysninger om nærmeste familie (navn, adresse og lignende), herunder formentlig også oplysninger om registreret partnerskab, skattemæssige oplysninger, bankoplysninger, oplysninger om pensionsforhold etc. Der kan også ske behandling af oplysninger om den ansattes uddannelse, tidligere beskæftigelse og andre sædvanlige oplysninger i et curriculum vitæ, anbefalinger etc. Endelig kan der være tale om oplysninger, der fremkommer under selve ansættelsesforholdet, f.eks. om nuværende stilling, arbejdsopgaver, arbejdstider og andre tjenstlige forhold, oplysninger om løn, skat, sygefravær og sygdomsperioder (oplysninger om antal sygedage betragtes normalt ikke som en helbredsoplysning), oplysninger om andet fravær fra arbejdet, tjenstlige forseelser og advarsler, personalebedømmelser og lignende. En arbejdsgiver må normalt registrere de oplysninger om en ansat, som den pågældende selv har afgivet i sin stillingsansøgning. [981]

10.4.2.1.2. Nærmere om behandling af følsomme oplysninger i forbindelse med personaleadministration

For så vidt angår følsomme oplysninger fremgår det at lov om behandling af personoplysninger med kommentarer[982], at et personaleregister i begrænset omfang kan indeholde følsomme oplysninger, jf. persondatalovens §§ 7 og 8, om de ansatte. Dette kan bl.a. kan dreje sig om oplysninger om helbredsforhold, herunder alkoholmisbrug, jf. § 7, stk. 2, oplysninger om medlemskab af en fagforening, jf. § 7, stk. 3, oplysninger om strafbare forhold samt andre tilsvarende rent private forhold, f.eks. bortvisning pga. grov tilsidesættelse af ansættelsesforholdet, jf. § 8, stk. 1 og 4. Det fremgår i øvrigt, at en arbejdsgivers oplysning om en positiv alkoholtest må anses for en rent privat oplysning, uanset at oplysningen ikke nødvendigvis dækker over et egentligt alkoholmisbrug, og at en personlighedstest og lignende som regel vil skulle betragtes som en følsom oplysning.

Det fremgår desuden af lov om behandling af personoplysninger med kommentarer[983], at en arbejdsgiver i praksis som hovedregel kun må registrere følsomme oplysninger om de ansatte, hvis de pågældende har givet samtykke dertil. Det er dog også muligt at registrere følsomme oplysninger i et personaleregister, hvis det er nødvendigt for arbejdsgiveren af hensyn til opfyldelsen af en regel i lov eller bekendtgørelse. F.eks. nødvendiggør funktionærloven i visse tilfælde registrering af følsomme oplysninger, bl.a. i tilfælde af opsigelse, hvor en ansats ret til på begæring at få oplysning om årsagen til afskedigelsen forudsætter registrering af oplysninger herom. Oplysninger om de ansattes fagforeningsmæssige tilhørsforhold kan indgå i et personaleregister, hvis betingelserne i persondatalovens § 7, stk. 3, er opfyldt. Behandling af oplysninger om strafbare forhold, f.eks. opbevaring af en straf-

[981] Persondataloven med kommentarer (2015), s 219.
[982] Persondataloven med kommentarer (2015), s 220.
[983] Persondataloven med kommentarer (2015), s 220.

feattest, skal ske efter reglerne i § 8, stk. 1 og 4. Herudover vil der kun være begrænset mulighed for at registrere følsomme oplysninger i et personaleregister. Der kan være tale om registrering, som er nødvendig for, at det kan fastlægges, om nogen har et retskrav, jf. § 7, stk. 2, nr. 4. Det vil f.eks. kunne forekomme, at en virksomhed kan registrere oplysninger om, at en ansat har begået et strafbart forhold over for virksomheden, hvis dette er nødvendigt for at kunne gøre virksomhedens krav på erstatning gældende mod den pågældende, jf. § 8, stk. 6. Også på områder, hvor der kan tænkes at opstå et retskrav for den ansatte, f.eks. et erstatningskrav som følge af en arbejdsskade, kan det være nødvendigt at foretage registrering af følsomme oplysninger til brug for en eventuel sag.[984]

Det fremgår desuden af Lov om behandling af personoplysninger med kommentarer[985], at bestemmelser i andre love kan begrænse adgangen til at indsamle, registrere eller i øvrigt behandle følsomme oplysninger, også selv om den registrerede har givet sit samtykke dertil. Dette vil efter omstændighederne kunne være tilfældet efter lov om brug af helbredsoplysninger mv. på arbejdsmarkedet, og lov om forbud mod forskelsbehandling pga. race mv.

10.4.2.2. Særligt om videregivelse af oplysninger om, at en person har søgt ansættelse hos en virksomhed

Datatilsynet har i forbindelse med beskæftigelsesministerens besvarelse af 25. august 2006 af spørgsmål nr. S 6697 udtalt, at det er Datatilsynets umiddelbare opfattelse, at en virksomhed (den dataansvarlige) ikke vil kunne videregive oplysninger om, at en person søger nyt arbejde til den pågældende persons nuværende arbejdsgiver efter interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7. Efter Datatilsynets opfattelse kan hensynet til virksomheden eller til arbejdsgiveren således ikke normalt antages at overstige personens interesse i, at den nuværende arbejdsgiver ikke bliver gjort bekendt med, at den pågældende – der sidder i uopsagt stilling – søger nyt arbejde. Videregivelse af oplysninger om, at en person søger nyt arbejde vil således efter tilsynets umiddelbare opfattelse normalt forudsætte et samtykke fra den pågældende person.

10.4.2.3. Særligt om offentliggørelse af medarbejderoplysninger

Efter Datatilsynets praksis må arbejdsgivere, private såvel som offentlige, offentliggøre arbejdsrelaterede oplysninger om ansatte på internettet uden forudgående samtykke med hjemmel i interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7. Datatilsynet har herved lagt vægt på, at offentliggørelse af sådanne oplysninger om ansatte er en naturlig del af en information om arbejdspladsen, samtidig med, at de ansatte normal ikke vil have indvendinger mod offentliggørelsen. Offentliggørelse af oplysninger af mere personlig karakter, f.eks. billede af den ansatte eller den ansattes private adresse, private e-

[984] Persondataloven med kommentarer (2015), s 220.
[985] Persondataloven med kommentarer (2015), s 221.

mailadresse eller et privat telefonnummer, kan dog alene offentliggøres med den ansattes samtykke.[986]

10.4.2.4. Særligt om videregivelse af medarbejderoplysninger til fagforeninger

Datatilsynet har i en række tilfælde forholdt sig til spørgsmål om videregivelse af oplysninger om ansatte til fagforeninger. Det fremgår af Lov om behandling af personoplysninger med kommentarer[987], at retsstillingen i lyset af Datatilsynets praksis kan sammenfattes således, at en dataansvarlig myndighed eller virksomhed uden samtykke kan videregive medarbejderoplysninger i form af identifikationsoplysninger, herunder personnumre, til en fagforening, som den pågældende er medlem af. Derimod kræver det som udgangspunkt samtykke fra den enkelte ansatte, hvis vedkommende ikke er medlem af fagforeningen. Dog kan videregivelse ske uden samtykke, hvis der foreligger særlige omstændigheder. Dette vil f.eks. være tilfældet, hvis videregivelsen har støtte i en overenskomst eller lignende med henblik på individuelle lønforhandlinger også for ikke-medlemmer. Det forudsættes naturligvis som betingelse for videregivelse uden samtykke, at kravene til saglighed og proportionalitet er opfyldt, jf. persondatalovens § 5, stk. 2 og 3. Videregivelse af personnumre for ansatte, der ikke er medlem af den pågældende fagforening, kræver dog under alle omstændigheder samtykke, jf. § 11, stk. 2, nr. 2.[988]

10.4.2.5. Særligt om videregivelse af oplysninger om ansattes løn

Datatilsynet har i en vejledende udtalelse fra 2007[989] skitseret rammerne for, hvornår der inden for rammerne af persondataloven kan ske videregivelse af oplysninger om ansattes løn. Udtalelsen er primært rettet mod det offentlige arbejdsmarked, idet det er Datatilsynets indtryk, at private arbejdspladser ofte har helt andre aftaler og traditioner for håndtering af lønoplysninger.

10.4.2.6. Kontrolforanstaltninger

Det fremgår af Lov om behandling af personoplysninger med kommentarer[990], at retsstillingen vedrørende kontrol med medarbejderes brug af hjemmesider og e-mail kan sammenfattes således: Såvel en offentlig myndighed som en privat virksomhed kan ud fra ledelses-, drifts- og sikkerhedsmæssige hensyn normalt foretage kontrol af, om fastsatte retningslinjer for brug af myndighedens eller virksomhedens edb-systemer bliver overholdt, jf. persondatalovens § 5, stk. 2, og § 6, stk. 1, nr. 7. Kontrollen kan rette sig mod medarbejdernes adgang til hjemmesider og afsendelse og modtagelse af private e-mails og kan omfatte en gennemgang af en eventuel sikkerhedskopi af ind- og udgående e-mails. Som

[986] Datatilsynets Årsberetning 2000, s. 33-35.
[987] Persondataloven med kommentarer (2015), s 233 f.
[988] Persondataloven med kommentarer (2015), s 233 f.
[989] Datatilsynets j.nr. 2007-321-0047.
[990] Persondataloven med kommentarer (2015), s 259 f.

udgangspunkt skal de ansatte på forhånd klart og tydeligt være gjort opmærksom på, at denne kontrol kan finde sted, jf. persondatalovens §§ 28 og 29 om oplysningspligt, og § 5, stk. 1, om god databehandlingsskik. Ved kontrol med e-mails må arbejdsgiver ikke læse indholdet af en e-mail, når denne er identificeret som privat, hvilket naturligvis også gør sig gældende, hvis der identificeres private e-mails i andre situationer end ved kontrol. Datatilsynet opfordrer i øvrigt til, at problemstillingen omkring privat udnyttelse af arbejdspladsens edb-systemer med internetadgang og adgangen til kontrol gøres til drøftelse i samarbejdsudvalg og lignende.[991]

10.4.3. Databeskyttelsesforordningen

10.4.3.1. Rum for fastsættelse af bestemmelser i national ret – artikel 88

Det fremgår af præambelbetragtning nr. 155, 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, og i forbindelse med ansættelse, ansættelseskontrakter, herunder godtgørelse for forpligtelser fastlagt ved lov eller kollektive overenskomster, ledelse, planlægning og tilrettelæggelse af arbejdet, ligestilling og mangfoldighed på arbejdspladsen, sikkerhed og sundhed på arbejdspladsen, individuel eller kollektiv udøvelse og nydelse af rettigheder og fordele i forbindelse med ansættelse samt ophør af ansættelsesforhold.

Det fremgår af 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 arbejdstagernes personoplysninger i ansættelsesforhold, navnlig med henblik på ansættelse, ansættelseskontrakter, herunder opfyldelse af forpligtelser fastsat ved lov eller i kollektive overenskomster, ledelse, planlægning og tilrettelæggelse af arbejdet, ligestilling og mangfoldighed på arbejdspladsen, arbejdsmiljø samt beskyttelse af arbejdsgiveres eller kunders ejendom og med henblik på individuel eller kollektiv udøvelse og nydelse af rettigheder og fordele i forbindelse med ansættelse samt med henblik på ophør af ansættelsesforhold.

Det fremgår af artikel 88, stk. 2, at disse bestemmelser skal omfatte passende og specifikke foranstaltninger til beskyttelse af den registreredes menneskelige værdighed, legitime interesser og grundlæggende rettigheder, særlig med hensyn til gennemsigtighed i behandlingen, overførsel af personoplysninger inden for en koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet, og overvågningssystemer på arbejdspladsen.

[991] Persondataloven med kommentarer (2015), s 260.

Det fremgår af artikel 88, stk. 3, at hver medlemsstat senest den 25. maj 2018 giver Kommissionen meddelelse om de (lov)bestemmelser, som den vedtager i henhold til stk. 1, og underretter den straks om alle senere ændringer, der berører dem.

10.4.3.2. Reguleringsform

Der henvises direkte i bestemmelsen i artikel 88, stk. 1, til, at medlemsstaterne ud over ved *lov* også i medfør af *kollektive overenskomster* kan fastsætte mere specifikke bestemmelser for at sikre beskyttelse af rettighederne og frihedsrettighederne i forbindelse med behandling af arbejdstagernes personoplysninger i ansættelsesforhold. Dette præciseres i præambelbetragtning nr. 155, at også bestemmelser i *"lokalaftaler"* skal henregnes til kollektive overenskomster.

10.4.3.3. Hjemmel til behandling af oplysninger

Det fremgår specifikt af forslaget til forordningens artikel 88 (forslagets artikel 82), at medlemslandene *under overholdelse af denne forordning* kan vedtage de omhandlede specifikke bestemmelser. Formuleringen er ikke medtaget i den endelige udgave af forordningens artikel 88, som dog i stk. 1 foreskriver, at bestemmelsen giver mulighed for at fastsætte "mere specifikke bestemmelser".

Artikel 88 omfatter alle typer af personoplysninger, nemlig de særlige kategorier af personoplysninger omfattet af artikel 9, stk. 1, og residual-mængden af oplysninger, dvs. personoplysninger omfattet af artikel 6. Denne opdeling af, hvad er der er "almindelige" personoplysninger og følsomme oplysninger, kan ikke ophæves ved brug af artikel 88, ligesom artikel 88 ikke ændrer på, at al behandling af personoplysninger skal være i overensstemmelse med de grundlæggende principper i forordningens artikel 5. Endelig ændrer artikel 88 ikke på, at kollektive overenskomster i øvrigt skal ligge indenfor rammerne af lovgivningen, jf. Jens Kristiansen, Grundlæggende arbejdsret, 4. udgave (2016), s. 30, om forholdet i dag mellem kollektive overenskomster og de ansættelsesretlige love.

Både artikel 6, stk. 2-3 og artikel 9, stk. 2, efterlader muligheder for at fastsætte nærmere nationale regler om behandling af personoplysninger, jf. afsnit 3.4. og 3.8. om disse bestemmelser. Det fremgår i den forbindelse specifikt af artikel 9, stk. 2, litra b, at behandling er lovlig, hvis den 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.

I forhold til mulighederne i artikel 6 og 9 for nationale lovregler og kollektive overenskomster om behandling af personoplysninger, må artikel 88 forstås som et hjemmelsmæssigt *supplement*, der sikrer, at der i hvert fald ikke er tvivl om, at der kan fastsættes nationale behandlingsregler i love og kollektive overenskomster på ansættelsesområdet for så vidt angår behandling af *alle* typer af personoplysninger – under overholdelse af kravene til sådan national lovgivning i f.eks. artikel 9, stk. 2, litra b, og artikel 88, stk. 2.

Artikel 88, stk. 1, oplister i den forbindelse en række *behandlingssituationer*, som de specifikke bestemmelser om behandling af arbejdstageres personoplysninger i ansættelsesforhold kan angå: Ansættelse, ansættelseskontrakter, herunder opfyldelse af forpligtelser fastsat ved lov eller i kollektive overenskomster, ledelse, planlægning og tilrettelæggelse af arbejdet, ligestilling og mangfoldighed på arbejdspladsen, arbejdsmiljø samt beskyttelse af arbejdsgiveres eller kunders ejendom og med henblik på individuel eller kollektiv udøvelse og nydelse af rettigheder og fordele i forbindelse med ansættelse samt med henblik på ophør af ansættelsesforhold. Denne oplistning suppleres af præambelbetragtning nr. 155, som i det væsentlige svarer til oplistningen i artikel 88, stk. 1.

For så vidt angår *ansættelse* fremgår det af den engelske sprogversion af forordningen, at der er tale om "recruitment", mens bestemmelsen i øvrigt angår "employment". Det må herefter lægges til grund, at muligheden for at fastsætte specifikke bestemmelser om "ansættelse" skal forstås således, at der kan fastsættes specifikke bestemmelser om *ansøgningsfasen*, dvs. inden ansættelse, hvor det f.eks. i praksis kan være relevant at indhente referencer fra tidligere arbejdsgivere.

10.4.3.4. Samtykke som behandlingsgrundlag

Det fremgår af forordningens præambelbetragtning nr. 155, 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, og i forbindelse med ansættelse, ansættelseskontrakter, herunder godtgørelse for forpligtelser fastlagt ved lov eller kollektive overenskomster, ledelse, planlægning og tilrettelæggelse af arbejdet, ligestilling og mangfoldighed på arbejdspladsen, sikkerhed og sundhed på arbejdspladsen, individuel eller kollektiv udøvelse og nydelse af rettigheder og fordele i forbindelse med ansættelse samt ophør af ansættelsesforhold.

Det må på denne baggrund antages, at forordningen efterlader rum for, at arbejdsgiveres behandling af personoplysninger i ansættelsesforhold, herunder i rekrutteringsfasen, fortsat

kan ske på grundlag af samtykke, jf. særligt artikel 6, stk. 1, litra a, og artikel 9, stk. 2, litra a.

10.4.3.5. Betingelser for fastsættelse af særlige behandlingsregler – passende og specifikke foranstaltninger

Bestemmelserne skal ifølge artikel 88, stk. 1, *sikre beskyttelse af rettighederne og frihedsrettighederne* i forbindelse med behandling af arbejdstagernes personoplysninger, og bestemmelserne skal ifølge artikel 88, stk. 2, omfatte *passende og specifikke foranstaltninger* til beskyttelse af den registreredes menneskelige værdighed, legitime interesser og grundlæggende rettigheder. Al national lovgivning og kollektive overenskomster om behandling af personoplysninger inden for området af artikel 88 skal leve op til betingelserne i artikel 88, stk. 2.

De passende og specifikke foranstaltninger skal særligt fastsættes med hensyn til *gennemsigtighed i behandlingen, overførsel af personoplysninger inden for en koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet, og overvågningssystemer på arbejdspladsen.*

10.4.3.6. Meddelelse til Kommissionen

Som det fremgår af artikel 88, stk. 3, skal hver medlemsstater senest den 25. maj 2018 give Kommissionen meddelelse om de "bestemmelser", som den vedtager i henhold til artikel 88, stk. 1, og straks underrette om alle senere ændringer, der berører dem.

Af den engelske sprogversion af forordningen fremgår det af artikel 88, stk. 3, at Kommissionen skal have meddelelse "of those provisions of its *law*". Det må på den baggrund antages, at stk. 3 alene forpligter medlemsstaterne til at give meddelelse til Kommissionen om *love* – og dermed ikke kollektive overenskomster – de måtte vedtage på området for artikel 88. Der er i den forbindelse også lagt vægt på den konsekvensbetragtning, at det ville savne praktisk mening, hvis Kommissionen straks skulle have meddelelse om enhver ændring af f.eks. enhver lokalaftale, der vedrører behandling af personoplysninger.

Der kan ikke antages at være pligt til at give Kommissionen meddelelse om allerede eksisterende lovgivning om behandling af personoplysninger i ansættelsesforhold. Artikel 88 er ny og tager sigte på fremtidig lovgivning.

10.4.3.7. Sammenfatning

Samlet set lader bestemmelsen i forordningens artikel 88 – sammen med artikel 6, stk. 2-3 og af artikel 9, stk. 2, litra b – det i vidt omfang være op til medlemsstaterne, om der skal ske særlig regulering af arbejdsgivernes behandling af de ansattes personoplysninger i for-

bindelse med ansættelsesforhold, og det overlades fuldt ud til medlemsstaterne at beslutte, om en eventuel nærmere reguleringen skal ske i form af lovgivning eller ved kollektive overenskomster. Som modvægt hertil skal der fastsættes passende og specifikke garantier, og Kommissionen skal holdes underrettet.

10.4.4. Overvejelser

Som anført ovenfor om gældende ret udfylder de arbejdsretlige normer de generelle regler i persondataloven. Behandling af ansattes personoplysninger i forbindelse med ansættelsesforhold skal således ske inden for rammerne af persondataloven, og indholdet af f.eks. kollektive overenskomster kan være af betydning ved vurdering af, om en given behandling er *nødvendig*.

Det må antages, at denne praksis, hvor arbejdsretlige normer spiller ind ved vurderingen af, om en behandling er *nødvendig*, kan videreføres også efter 25. maj 2018, idet der *f.eks.* i forordningens artikel 6, stk. 1, litra b og 6, stk. 2-3, gives mulighed for at behandle oplysninger, hvis det er *nødvendigt* af hensyn til opfyldelsen af en kontrakt, som den registrerede er part i, og i artikel 9, stk. 2, litra b, at behandling er lovlig, hvis den 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 frihedsrettigheder.

I forhold til mulighederne i artikel 6 og 9 for nationale lovregler og kollektive overenskomster om behandling af personoplysninger må artikel 88 forstås som et hjemmelsmæssigt *supplement*, der sikrer, at der i hvert fald ikke er tvivl om, at der kan fastsættes nationale behandlingsregler på ansættelsesområdet for så vidt angår behandling af *alle* typer af personoplysninger – under overholdes af kravene til sådan national lovgivning i f.eks. artikel 9, stk. 2, litra b, og artikel 88, stk. 2.

Desuden vil den behandling af oplysninger om ansatte i forbindelse med arbejdsforhold, som efter nuværende praksis kræver samtykke, også efter 25. maj 2018 kunne ske på grundlag af samtykke.

10.5. Rammerne i artikel 89, stk. 1 og 2 samt 4, vedrørende videnskabelige og historiske forskningsformål og statistiske formål

10.5.1. Præsentation

Databeskyttelsesforordningens artikel 89, stk. 1, indeholder en særlig regel, hvorefter behandling af personoplysninger til bl.a. videnskabelige og historiske forskningsformål og statistiske formål, skal være underlagt fornødne garantier for de registreredes rettigheder og frihedsrettigheder.

Endvidere skal medlemsstaterne ved fastsættelse af nationale særregler på baggrund af forordningens artikel 9, stk. 2, litra j, hvorefter behandling er lovlig, hvis behandlingen 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, sikre de fornødne garantier for de registreredes rettigheder og frihedsrettigheder i medfør af artikel 89, stk. 1.

Herudover er det muligt efter forordningens artikel 89, stk. 2, at fastsætte nationale særregler, der undtager fra de registreredes rettigheder, når der behandles oplysninger til disse formål.

10.5.2. Gældende ret

Der henvises til afsnit 3.2. om forskning og statistik for en nærmere gennemgang af gældende ret.

For så vidt angår behandling efter gældende ret af personoplysninger om afdøde personer, skal det bemærkes, at det fremgår af bemærkningerne til persondataloven, at oplysninger om afdøde personer skal anses for personoplysninger og dermed være omfattet af lovens regulering.[992]

Det betyder, at allerede behandlede oplysninger, efter personens død fortsat vil være omfattet af loven, hvis der ud fra en konkret vurdering fortsat er et beskyttelseshensyn. Dette indebærer også, at indsamling og efterfølgende behandling af oplysninger om afdøde skal opfylde lovens betingelser, hvis der foreligger et særligt beskyttelsesbehov.

[992] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.2.3. i de almindelige bemærkninger.

Det fremgår endvidere af bemærkningerne til persondataloven, at det overlades til tilsynsmyndighederne at fastlægge de nærmere grænser for persondatalovens anvendelse på oplysninger om afdøde personer.

10.5.3. Databeskyttelsesforordningen

10.5.3.1. Fornødne garantier efter artikel 89, stk. 1

Det følger af databeskyttelsesforordningens artikel 89, stk. 1, at behandling til bl.a. videnskabelige eller historiske forskningsformål eller til statistiske formål skal 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 disse formål kan opfyldes ved viderebehandling, som ikke gøre det muligt eller ikke længere gør det muligt at identificere de registrerede, skal formålene opfyldes på denne måde.

Det følger i den forbindelse af præambelbetragtning nr. 156, at de pågældende garantier kan indebære specifikke procedurer for registreredes udøvelse af deres rettigheder, hvis dette er relevant i lyset af de formål, der tilstræbes med den specifikke behandling. Herudover fremgår det af betragtningen, at også tekniske og organisatoriske foranstaltninger med henblik på at minimere behandling af personoplysninger i medfør af proportionalitetsprincippet og nødvendighedsprincippet, kan udgøre fornødne garantier.

Foruden disse, følger det af præambelbetragtning nr. 159, at der bør gælde særlige betingelser navnlig for offentliggørelse eller anden fremlæggelse af personoplysninger i forbindelse med videnskabelige forskningsformål.

For så vidt angår statistiske formål, følger det af præambelbetragtning nr. 162, 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.

10.5.3.1.1. Rammer for nationale særregler på baggrund af artikel 9, stk. 2, litra j

Forordningens artikel 9, stk. 2, litra j, om behandling af følsomme oplysninger, giver adgang til at behandle oplysninger 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*.

Ved fastsættelsen af nationale særregler på baggrund af forordningens artikel 9, stk. 2, litra j, skal medlemsstaterne således fastsætte de fornødne garantier for de registreredes rettigheder og frihedsrettigheder i medfør af artikel 89, stk. 1.

Det må antages, at artikel 89, stk. 1, skal anses som en understregning af, at der ved fastsættelse af nationale særregler om behandling til videnskabelige og historiske forskningsformål samt statistiske formål på baggrund af artikel 9, stk. 2, litra j, skal sikres de fornødne garantier i den pågældende nationale særregel. Dermed ses artikel 89, stk. 1, ikke direkte at pålægge yderligere forpligtelser, udover hvad der allerede kræves efter forordningens artikel 9, stk. 2, litra j.

10.5.3.1.2. Overvejelser om videreførelse af persondatalovens § 10, stk. 1

Det følger af persondatalovens § 10, stk. 1, at oplysninger som nævnt i lovens § 7, stk. 1, eller § 8 må behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for udførelsen af undersøgelserne.

Der gives således en lempeligere adgang til at behandle følsomme oplysninger, der alene behandles i statistisk eller videnskabeligt øjemed.

Det bemærkes, at historiske forskningsformål ikke udtrykkeligt er omfattet af bestemmelsens ordlyd. Registerudvalget anførte imidlertid i betænkning nr. 1345, at udtrykkene "statistiske eller videnskabelige undersøgelser", skal forstås således, at der er tale om en videnskabelig bearbejdning af oplysninger som led i en undersøgelse eller statistisk belysning.[993] Behandling til historiske forskningsformål må således anses for indeholdt i betegnelsen "videnskabelige undersøgelser" efter persondatalovens § 10.

Der er i persondatalovens § 10 fastsat fornødne garantier mod misbrug af de behandlede oplysninger, med henblik på at efterleve kravet til at kunne undtage fra forbuddet om behandling af følsomme oplysninger i medfør af artikel 8, stk. 4, i databeskyttelsesdirektivet.

Efter persondatalovens § 10, stk. 1, finder bestemmelsen således kun anvendelse, når oplysningerne *alene* behandles med henblik på at udføre undersøgelser af *væsentlige samfundsmæssig betydning*.

Bestemmelsen har et snævert anvendelsesområde, idet en behandling ikke samtidig må have andre formål end statistiske og forskningsmæssige. Såfremt dette er tilfældet, kan §

[993] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 253.

10 ikke anvendes, og behandlingsgrundlagene i persondatalovens §§ 7 og 8 finder i stedet anvendelse.

Det følger endvidere af persondatalovens § 10, stk. 1, at det er et krav, *at* behandlingen er *nødvendig* for udførelsen af undersøgelserne. Der er her tale om en foranstaltning i medfør af nødvendighedsprincippet, som også nævnes i databeskyttelsesforordningens præambelbetragtning nr. 156, som en foranstaltninger, der kan udgøre garantier for de registreredes rettigheder og frihedsrettigheder efter forordningens artikel 89, stk. 1.

Det vurderes på den baggrund, at en videreførelse af persondatalovens § 10, stk. 1, kan udgøre et element til at sikre, at der fastsættes fornødne garantier i overensstemmelse med databeskyttelsesforordningens artikel 89, stk. 1, og i øvrigt også artikel 9, stk. 2, litra j.

10.5.3.1.3. Overvejelser om videreførelse af persondatalovens § 10, stk. 2

Det følger af persondatalovens § 10, stk. 2, at oplysninger omfattet af bestemmelsens stk. 1, ikke senere må behandles til andre formål end statistiske og videnskabelige. Dette medfører bl.a., at oplysninger behandlet på baggrund af persondatalovens § 10, stk. 1, heller ikke efterfølgende må anvendes til andre formål, såsom journalistiske mv.[994] eller til at træffe konkrete afgørelser eller andre konkrete foranstaltninger over for de registrerede.[995]

Persondatalovens § 10 giver mulighed for at behandle oplysninger, uden at de registrerede har samtykket til den pågældende behandling af deres oplysninger. Det må antages at udgøre en fornøden garanti for de registreredes rettigheder, at der med formålsbegrænsningen i lovens § 10, stk. 2, fastsættes, at oplysningerne *ikke* kan behandles til andre formål. Herudover følger det af Datatilsynets praksis, at bestemmelsen må antages udtømmende at have gjort op med mulighederne for videregivelse, herunder at den ikke kan suppleres med samtykkeregler i persondataloven.[996]

Formålsbegrænsningen i persondatalovens § 10, stk. 2, kan derfor antages at udgøre en garanti for de registreredes rettigheder og frihedsrettigheder, som er inden for rammerne af forordningens artikel 89, stk. 1.

[994] Datatilsynets afgørelse, j.nr. 2002-41-2492
[995] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 257.
[996] Datatilsynets j.nr. 2002-216-0096 gengivet i tilsynets årsberetning 2002, s. 68-69.

Herudover skal det bemærkes, at det følger af forarbejderne til persondatalovens § 10, stk. 2, at der i formålsbegrænsningen ligger, at en undersøgelse ikke må offentliggøres på en sådan måde, at det er muligt at identificere den enkelte registrerede.[997]

Denne garanti må ligeledes anses for at være inden for rammerne af forordningens artikel 89, stk. 1, herunder særlig 3. pkt. i bestemmelsen om, at når disse formål 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. Dette fremgår også af forordningens præambelbetragtning nr. 159, hvorefter der bør gælde særlige betingelser navnlig for offentliggørelse eller anden fremlæggelse af personoplysninger i forbindelse med videnskabelige forskningsformål.

For så vidt angår formålsbegrænsningen i persondatalovens § 10, stk. 2, skal det endvidere undersøges, hvorvidt denne særlige garanti i sin helhed kan holdes inden for rammerne af forordningens artikel 89, stk. 1.

Det følger af forordningens artikel 89, stk. 4, at når behandling, som omhandlet i stk. 2 og 3, samtidig tjener et andet formål, anvendes undtagelser (til de registreredes rettigheder) kun til de arkivformål i samfundets interesse, videnskabelige og historiske forskningsformål og statistiske formål, der er omhandlet i nævnte stykker.

Bestemmelsen *kan* på baggrund af sin ordlyd antages at indeholde en forudsætning om mulighed for samtidig behandling til andre end videnskabelige eller historiske forskningsformål eller statistiske.

Det følger i den forbindelse af forordningens præambelbetragtning nr. 159, at hvis resultatet af videnskabelig forskning navnlig inden for sundhed giver grund til yderligere foranstaltninger i den registreredes interesse, bør de generelle regler i forordningen finde anvendelse med henblik på disse foranstaltninger.

For så vidt angår behandling i statistik øjemed, kan det endvidere bemærkes, at det i præambelbetragtning nr. 162, anføres, at det statistiske formål indebærer, at resultatet af behandling til statistiske formål ikke er personoplysninger, men aggregerede data, og at dette resultat eller personoplysninger ikke anvendes til støtte for foranstaltninger eller afgørelser, der vedrører bestemte fysiske personer.

[997] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 10.

Der er ikke faste holdepunkter i ordlyden af artikel 89, stk. 4, for at antage, at det ikke er *muligt* at fastsætte en garanti for de registreredes rettigheder og frihedsrettigheder i medfør af artikel 89, stk. 1, svarende til den, der følger af formålsbegrænsningen i persondatalovens § 10, stk. 2, hvis det er det medlemsstaterne ønsker. Artikel 9, stk. 2, litra j, overlader det netop udtrykkeligt til medlemsstaterne at bestemme, hvad "passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser" er. Det bemærkes i den forbindelse, at § 10, stk. 2, er tiltænkt som en opfyldelse af databeskyttelsesdirektivets artikel 8, stk. 4, der kræver "tilstrækkelige garantier", jf. Registerudvalgets betænkning 1345, s. 257.

Det bemærkes i den forbindelse også, at andre dataansvarlige, der ikke behandler oplysninger efter persondatalovens § 10, kan behandle de pågældende oplysninger til andre formål efter persondatalovens §§ 6-8.

På baggrund af forordningens ordlyd vurderes det således, at den danske særregel om formålsbegrænsning i persondatalovens § 10, stk. 2, kan videreføres inden for rammerne af artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j.

Der er omvendt også holdepunkter for at antage, at der for eksempel kan fastsættes nationale særregler, som muliggør videre behandling til brug for andre formål end videnskabelige og historiske forskningsformål og statistiske formål af de pågældende oplysninger på baggrund af den registreredes samtykke efter forordningens regler.

På samme måde er der endvidere holdepunkter for at antage, at der for eksempel også kan fastsættes en national særregel, som alene gør det muligt at foretage videre behandling til andre formål end videnskabelige og historiske forskningsformål og statistiske formål under særlige omstændigheder, herunder hensynet til den registreredes (vitale) interesser.

10.5.3.1.4. Overvejelser om videreførelse af persondatalovens § 10, stk. 3 (tilladelse til videregivelse)

Det følger af den nationale særregel i persondatalovens § 10, stk. 3, at der skal indhentes tilladelse fra Datatilsynet forud for videregivelse af oplysninger omfattet af § 10, stk. 1 og 2, til tredjemand.

Registerudvalget anførte i betænkning nr. 1345, at udvalget anså tilladelsesordningen som et element i at sikre, at der i dansk ret blev stillet de i databeskyttelsesdirektivet krævede fornødne garantier mod misbrug af de behandlede oplysninger, hvilket også må antages at

være inden for rammerne af garantier i forordningens artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j.[998]

Hertil skal det bemærkes, at der i forordningens artikel 36, stk. 5, er mulighed for, at det i medlemsstaternes nationale ret kan kræves, at dataansvarlige hører og opnår forudgående tilladelse fra tilsynsmyndigheden i forbindelse med den dataansvarliges behandling under udførelsen af en opgave i samfundets interesse, herunder behandling i forbindelse med social sikring og folkesundhed.

Idet behandling til historiske og videnskabelige forskningsformål og statistiske formål må anses som udførelse af en opgave i samfundets interesse, må det antages, at en tilladelsesordning svarende til den i persondatalovens § 10, stk. 3, også kan rummes inden for rammerne af forordningens artikel 36, stk. 5. Der henvises i øvrigt til afsnit 5.14. om artikel 36.

10.5.3.1.5. Anmeldelsesordning

Det må ligeledes antages, at en anmeldelsesordning, hvorefter tilsynsmyndigheden på visse vilkår og betingelser kan give forudgående tilladelse til en behandling af personoplysninger, kan udgøre en garanti for de registreredes rettigheder og frihedsrettigheder inden for rammerne af forordningens artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j.

10.5.3.2. Rammer for nationale særregler efter artikel 89, stk. 2

Det følger af forordningens artikel 89, stk. 2, at når personoplysninger behandles til *videnskabelige eller historiske forskningsformål eller til statiske formål*, kan EU-retten eller medlemsstaternes nationale ret fastsætte undtagelser fra de rettigheder, der er omhandlet i artikel 15 (*retten til indsigt*), 16 (*ret til berigtigelse*), 18 (*ret til begrænsning af behandling*) og 21 (*ret til indsigelse*), under iagttagelse af de betingelser og garantier, der er omhandlet i artikel 89, 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.

Fastsættelsen af nationale særregler, der undtager visse af de registrerede rettigheder, når der behandles oplysninger efter disse formål, beror således på en konkret afvejning fra lovgivers side af, om det kan sandsynliggøres, at sådanne rettigheder vil gøre det umuligt eller i alvorlig grad hindre opfyldelse af de specifikke formål, og sådanne undtagelser er nødvendige for at opfylde formålene.

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

Efter gældende ret begrænses retten til indsigt for så vidt angår oplysninger, der udelukkende behandles i videnskabeligt øjemed, eller for så vidt angår oplysninger behandlet i statistisk øjemed, hvor oplysningerne kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker efter persondatalovens § 32, stk. 4.

Det må antages, at denne nationale særregel, som undtager fra retten til indsigt efter databeskyttelsesforordningens artikel 15, er inden for rammerne af forordningens artikel 89, stk. 2.

Databeskyttelsesdirektivets artikel 12, litra b, og persondatalovens § 37, regulerer ret til bl.a. berigtigelse og blokering af oplysninger, som overordnet svarer til henholdsvis databeskyttelsesforordningens artikel 16 og 18. Der er ikke efter gældende ret i persondatalovens § 37 en undtagelse til retten til berigtigelse for behandling til historiske eller videnskabelige forskningsformål eller statistiske formål.

Det er således efter forordningens artikel 89, stk. 2, muligt at fastsætte nationale særregler, der udvider de gældende undtagelser til de registreredes rettigheder til retten til berigtigelse efter forordningens artikel 16 og retten til begrænsning af behandling efter artikel 18, når der behandles oplysninger i forskningsmæssig eller statistisk øjemed. Fastsættelsen af yderligere undtagelser til de registreredes rettigheder skal som sagt være baseret på en konkret vurdering af nødvendigheden heraf.

For så vidt angår retten til indsigelse efter forordningens artikel 21, er den altovervejende hovedregel i gældende ret, at retten til indsigelse ikke tages til følge, hvis der er tale om en behandling i statistisk eller videnskabeligt øjemed.[999] Det må således antages, at praksis kan videreføres inden for rammerne af forordningens artikel 89, stk. 2.

For så vidt angår den dataansvarliges oplysningspligt efter forordningens artikel 14, når personoplysningerne ikke er indsamlet hos den registrerede, fastsættes der i bestemmelsens stk. 5, litra b, en undtagelse, som omfatter 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. Hertil kræves, at meddelelse af sådanne oplysninger viser sig umulig eller vil kræve en uforholdsmæssigt stor indsats, eller i det omfang oplysningsforpligtelsen sandsynligvis vil gøre det umuligt eller i alvorlig grad vil hindre opfyldelse af formålene med behandlingen. Forordningens undtagelsesmulighed anses desuden for at være en videreførelse af gældende ret.

[999] Datatilsynets vejledning om de registreredes rettigheder, afsnit 4.1.

For så vidt angår den registreredes ret til sletning efter forordningens artikel 17, finder bestemmelsen ikke anvendelse i det omfang, behandlingen er nødvendig til videnskabelige eller historiske forskningsformål eller statistiske formål i overensstemmelse med artikel 89, stk. 1, og i det omfang retten til sletning sandsynligvis vil gøre det umuligt eller i alvorlig grad hindre opfyldelse af denne behandling, jf. artikel 17, stk. 3, litra d.

10.5.3.3. Artikel 89, stk. 4

Det følger af forordningens artikel 89, stk. 4, at når behandling som omhandlet i stk. 2 og 3 samtidig tjener et andet formål, anvendes undtagelser (til de registreredes rettigheder) kun til de arkivformål i samfundets interesse, videnskabelige og historiske forskningsformål og statistiske formål, der er omhandlet i nævnte stykker.

10.5.4. Overvejelser

Medlemsstaternes mulighed for at opretholde nationale særregler, som opstiller betingelser, der skal sikre fornødne garantier for de registreredes rettigheder og frihedsrettigheder ved behandling af oplysninger til historiske eller videnskabelige forskningsformål eller statistiske formål, vil overordnet ikke være en ændring i forhold til gældende ret.

For så vidt angår videreførelsen af gældende ret, må det antages, at persondatalovens § 10 i sin helhed kan videreføres inden for rammerne af artikel 89, stk. 1 og artikel 9, stk. 2, litra j.

Det skal hertil bemærkes, at det endvidere er muligt at fastsætte nationale særregler inden for rammerne af forordningen, hvorefter der kan ske videre behandling til andre formål end videnskabelige eller historiske forskningsformål f.eks. på baggrund af samtykke fra den registrerede eller ved særlige omstændigheder, herunder hensynet til den registreredes (vitale) interesser.

Herudover er det efter forordningens artikel 89, stk. 2, muligt at fastsætte nationale særregler, der undtager for de registreredes rettigheder, når der behandles oplysninger til disse formål, der både gør det muligt at videreføre gældende undtagelser samt udvide disse.

Det skal overvejes, om oplysninger om afdøde personer skal være omfattet af eventuelle nationale regler om behandling af personoplysninger til videnskabelige eller historiske forskningsformål eller til statistiske formål, jf. præambelbetragtning 27, hvorefter medlemsstaterne kan fastsætte regler for behandling af personoplysninger om afdøde personer.

Hvis medlemsstaterne ikke fastsætter regler herom, finder forordningen ikke anvendelse på personoplysninger om afdøde personer, jf. præambelbetragtning nr. 27, 158 og 160.

10.6. Rammerne i artikel 89, stk. 1 og 3 samt 4, vedrørende arkivformål i samfundets interesse

10.6.1. Præsentation

Efter databeskyttelsesforordningens artikel 9, stk. 2, litra j, kan der i overensstemmelse med artikel 89, stk. 1, fastsættes nationale særregler for så vidt angår behandling af følsomme oplysninger til bl.a. arkivformål i samfundets interesse.

Det følger af forordningens artikel 89, stk. 1, at behandling til bl.a. arkivformål i samfundets interesse skal være underlagt fornødne garantier for de registreredes rettigheder og frihedsrettigheder i overensstemmelse med forordningen.

Dernæst er det muligt at fastsætte nationale særregler, som undtager fra visse af de registreredes rettigheder, når dette anses for nødvendigt for at behandle oplysninger til arkivformål i samfundets interesse efter artikel 89, stk. 3.

Endelig følger det af artikel 89, stk. 4, at disse undtagelser alene gælder den del af behandlingen, som er til arkivformål i samfundets interesse.

10.6.2. Gældende ret

Det følger af persondatalovens § 14, at oplysninger, der er omfattet af denne lov, kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Registerudvalget anførte i betænkning nr. 1345, at der ved udformningen af bestemmelsen blev lagt vægt på, at lovtekniske hensyn tilsagde, at der burde skabes klarhed om reglerne om arkivering af personoplysninger mv.[1000]

Det fremgår herudover af bemærkningerne til persondataloven, at persondatalovens § 14 bygger på den forudsætning, at spørgsmålet om arkivmæssig anvendelse af personoplysninger afgøres efter arkivlovgivningens regler herom, og dermed ikke efter reglerne i persondatalovens kapitel 4 om behandling af oplysninger.[1001]

[1000] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 166.
[1001] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.11.3. i de almindelige bemærkninger.

Det fremgår endvidere af bemærkningerne til persondataloven, at de øvrige generelle regler i persondataloven finder anvendelse på arkivmæssig behandling af personoplysninger, medmindre det databeskyttelsesretlige spørgsmål er reguleret i arkivlovgivningen.

Det fremgår desuden af bemærkningerne til lov om offentlige arkiver (arkivloven), at forholdet til persondatalovens regler bl.a. indebærer, at de regler i persondataloven, der vedrører anmeldelse til Datatilsynet af behandling af personoplysninger samt registreredes rettigheder, som udgangspunkt finder anvendelse på arkivernes behandling af personoplysninger.[1002]

For så vidt angår retten til indsigt, er der i arkivlovens § 42 fastsat særlige regler for proceduren i forbindelse med begæring om indsigt i oplysninger, der er overført til opbevaring i arkiv. Selve vurderingen af den registreredes ret til indsigt i oplysninger, der er overført til opbevaring i arkiv vurderes fortsat efter reglerne i persondataloven.[1003]

Herudover finder de registreredes øvrige rettigheder efter persondatalovens regler anvendelse ved behandling til arkivmæssige formål.

Det bemærkes, at det fremgår af bemærkningerne til persondataloven, at oplysninger om afdøde personer skal anses for personoplysninger og dermed omfattet af lovens regulering.[1004] Det betyder, at allerede behandlede oplysninger efter personens død fortsat vil være omfattet af loven, hvis der ud fra en konkret vurdering fortsat er et beskyttelseshensyn. Dette indebærer også, at indsamling og efterfølgende behandling af oplysninger om afdøde skal opfylde lovens betingelser, hvis der foreligger et særligt beskyttelsesbehov.

Det fremgår endvidere af bemærkningerne til persondataloven, at det overlades til tilsynsmyndighederne at fastlægge de nærmere grænser for persondatalovens anvendelse på oplysninger om afdøde personer.

10.6.3. Databeskyttelsesforordningen

10.6.3.1. Rammerne for nationale særregler til arkivformål i samfundets interesse på baggrund af artikel 9, stk. 2, litra j, i overensstemmelse med artikel 89, stk. 1

Rammen for at fastsætte nationale særregler vedrørende arkivformål i samfundets interesse følger af databeskyttelsesforordningens artikel 9, stk. 2, litra j. På baggrund af forordnin-

[1002] Forslag nr. L 153 fremsat 15. december 1999, FT 1999/00, til lov om offentlige arkiver mv., almindelige bemærkninger.
[1003] Forslag nr. L 153 fremsat 15. december 1999 til lov om offentlige arkiver mv., de specielle bemærkninger til § 32 a (nuværende § 42).
[1004] Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, afsnit 4.2.2.3. i de almindelige bemærkninger.

gens generelle formål, ordlyden i forordningens artikel 9, stk. 2, litra j, samt de tilknyttede præambelbetragtninger er der ikke indikationer for, at det har været hensigten med bestemmelsen, at der med databeskyttelsesforordningen er tiltænkt et andet rum end direktivets for at fastsætte nationale regler i forbindelse med behandling af følsomme oplysninger, hvorfor det nationale råderum på disse område er en videreførelse af gældende ret. Der henvises i den forbindelse til afsnit 3.8. om artikel 9, stk. 2.

Ved fastsættelsen af nationale særregler om behandling af personoplysninger til arkivformål i samfundets interesse på baggrund af forordningens artikel 9, stk. 2, litra j, skal medlemsstaterne fastsætte fornødne garantier for de registreredes rettigheder og frihedsrettigheder i medfør af artikel 89, stk. 1.

Det må antages, at artikel 89, stk. 1, skal anses som en understregning af, at der ved fastsættelse af nationale særregler om behandling til bl.a. arkivformål i samfundets interesse på baggrund af artikel 9, stk. 2, litra j, skal sikres de fornødne garantier i den pågældende nationale særregel. Dermed ses artikel 89, stk. 1, ikke direkte at pålægge yderligere forpligtelser, udover hvad der allerede kræves efter forordningens artikel 9, stk. 2, litra j.

Det følger af artikel 89, stk. 1, at behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statiske formål skal 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 – hvor der altså stadig er tale om personoplysninger i forordningens forstand – forudsat at disse formål kan opfyldes på denne måde. Når disse formål 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.

Det følger desuden af præambelbetragtning nr. 158, at når der behandles oplysninger til arkivformål, bør forordningen også gælde for den pågældende behandling, idet forordningen dog ikke bør finde anvendelse på afdøde personer.

Det må på baggrund af artikel 89, stk. 1, suppleret af præambelbetragtning nr. 158, antages, at den gældende systematik, hvorved behandling til arkivmæssige formål afgøres efter arkivloven, og at databeskyttelseslovgivningen i øvrigt finder anvendelse, medmindre det databeskyttelsesretlige spørgsmål er reguleret i arkivloven, kan videreføres inden for rammerne af forordningen.

Dog skal det bemærkes, at forordningens regler ikke finder anvendelse for så vidt angår behandlingen af oplysninger om afdøde personer, men medlemsstaterne kan selv fastsætte regler om behandling af personoplysninger om sådanne personer, jf. præambelbetragtning nr. 27.

Det følger endvidere af præambelbetragtning nr. 158, at offentlige myndigheder eller offentlige eller private organer, der opbevarer fortegnelser af samfundsinteresse, bør være tjenester, der i henhold til EU-retten eller medlemsstaternes nationale ret har retlig forpligtelse til at indhente, bevare, vurdere, ordne, beskrive, udlevere, fremme, formidle og give adgang til fortegnelser af blivende værdi i samfundets interesse.

Det må således antages, at sådanne forpligtelser bl.a. bør fremgå af den nationale særregel om behandling af oplysninger til arkivformål i samfundets interesse for, at denne kan anses for at være inden for rammerne af forordningens artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j.

Det følger desuden af præambelbetragtning nr. 158, at medlemsstaterne bør have tilladelse til at fastsætte, at personoplysninger kan viderebehandles til arkivformål, f.eks. for at tilvejebringe specifikke oplysninger om politisk adfærd under tidligere totalitære regimer, folkedrab, forbrydelser mod menneskeheden, navnlig holocaust, eller krigsforbrydelser.

Det må derfor endvidere antages, at der skal tilvejebringes en sådan behandlingsmulighed i den nationale særregel om behandling af oplysninger til arkivformål i samfundets interesse for, at denne kan anses for at være inden for rammerne af forordningens artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j.

Herudover skal det bemærkes, at fastsættelsen af nationale særregler med *længerevarende* tilgængelighedsfrister for arkivenheder, der indeholder oplysninger om enkeltpersoners private forhold, må antages at kunne udgøre et element til at sikre, at der fastsættes fornødne garantier, herunder organisatoriske foranstaltninger, i medfør af artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j.

Det samme må antages at gøre sig gældende for nationale særregler, der alene muliggør behandling af arkivenheder, der indeholder oplysninger om enkeltpersoners private forhold, *før* den længerevarende tilgængelighedsfrist er udløbet, når forholdene taler herfor, og der foretages forudgående høring af tilsynsmyndighederne i de tilfælde, hvor oplysningerne er omfattet af databeskyttelseslovgivningen.

10.6.3.2. Rammerne for nationale særregler, der undtager for de registreredes rettigheder
Det følger af forordningens artikel 89 stk. 3, at når personoplysninger behandles til *arkivformål i samfundets interesse*, kan EU-retten eller medlemsstaternes nationale ret fastsætte undtagelser fra de rettigheder, der er omhandlet i artikel 15 (*indsigtsret*), 16 (*ret til berigtigelse*), 18 (*ret til begrænsning af behandling*), 19 (*underretningspligt*), 20 (*ret til dataportabilitet*) og 21 (*ret til indsigelse*), under iagttagelse af de betingelser og garantier, der er omhandlet i artikel 89, 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.

Det må antages, at den særlige regel for proceduren ved indsigt efter arkivlovens § 42 vil kunne videreføres efter forordningens artikel 89, stk. 3.

Det er således på baggrund af forordningens artikel 89, stk. 3, muligt at fastsætte undtagelser til hhv. forordningens artikel 15, 16, 18, 19, 20 og 21, såfremt det konkret vurderes nødvendigt at undtage disse rettigheder for at kunne behandle oplysninger til arkivformål i samfundets interesse.

Fastsættelsen af nationale særregler, der undtager visse af de registrerede rettigheder, når der behandles oplysninger til arkivformål i samfundets interesse, beror på en konkret afvejning fra lovgivers side af, om det kan sandsynliggøres, at sådanne rettigheder vil gøre det umuligt eller i alvorlig grad hindre opfyldelse af det specifikke formål, og sådanne undtagelser er nødvendige for at opfylde formålet.

For så vidt angår den dataansvarliges oplysningspligt efter forordningens artikel 14, fastsættes der i bestemmelsens stk. 5, litra b, en undtagelse, som omfatter behandling, der foretages til bl.a. arkivformål i samfundets interesse, og som overholder de fornødne garantier for registreredes rettigheder og frihedsrettigheder, der følger af forordningens artikel 89, stk. 1. Hertil kræves, at meddelelse af sådanne oplysninger viser sig umulig eller vil kræve en uforholdsmæssigt stor indsats, eller i det omfang oplysningsforpligtelsen sandsynligvis vil gøre det umuligt eller i alvorlig grad vil hindre opfyldelse af formålene med behandlingen. Der henvises til afsnit 4.4. om oplysningspligt, artikel 14.

For så vidt angår den registreredes ret til sletning efter forordningens artikel 17, finder bestemmelsen ikke anvendelse i det omfang, behandlingen er nødvendig til arkivformål i samfundets interesse i overensstemmelse med artikel 89, stk. 1, og i det omfang retten til sletning sandsynligvis vil gøre det umuligt eller i alvorlig grad hindre opfyldelse af denne behandling, jf. artikel 17, stk. 3, litra d.

10.6.3.3. Artikel 89, stk. 4

Det følger af stk. 4, at når behandling som omhandlet i stk. 2 og 3 samtidig tjener et andet formål, anvendes undtagelser kun til de formål, der er omhandlet i nævnte stykker.

10.6.4. Overvejelser

I det omfang der er fastsat de fornødne garantier i de nationale særregler om behandling af oplysninger til arkivformål i samfundets interesse i medfør af forordningens artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j, kan disse videreføres inden for rammerne af forordningen.

Det kan desuden antages, at den gældende forudsætning for forholdet mellem persondataloven og arkivlovens regler vil kunne videreføres inden for rammerne af forordningens artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j.

Det er endvidere muligt at fastsætte undtagelser til de registreredes rettigheder, når der behandles oplysninger til arkivformål i samfundets interesse, såfremt dette vurderes nødvendigt efter forordningens artikel 89, stk. 3.

Det skal overvejes, om oplysninger om afdøde personer skal være omfattet af eventuelle nationale regler om behandling af personoplysninger til videnskabelige eller historiske forskningsformål eller til statistiske formål, jf. præambelbetragtning 27, hvorefter medlemsstaterne kan fastsætte regler for behandling af personoplysninger om afdøde personer.

Hvis medlemsstaterne ikke fastsætter regler herom, finder forordningen ikke anvendelse på personoplysninger om afdøde personer, jf. præambelbetragtning nr. 27, 158 og 160.

10.7. Rammerne i artikel 90 for nationale regler om tilsynsmyndighedernes adgang til oplysninger, som er underlagt tavshedspligt

10.7.1. Præsentation

Med forordningens artikel 90 gives medlemsstaterne mulighed for at fastsætte specifikke regler med henblik på at sikre adgang til oplysninger, som er underlagt tavshedspligt, i de situationer, hvor tilsynsmyndighederne er beføjede til at få adgang til *oplysninger* og *lokaler mv*. hos den dataansvarlige eller hos databehandleren.

I det følgende vil rammerne for fastsættelse af nationale særregler i relation til tilsynsmyndighedernes beføjelser vedrørende oplysninger, som er underlagt tavshedspligt, blive gennemgået. For en nærmere gennemgang af tilsynsmyndighedernes beføjelser henvises til afsnit 7.7. om artikel 58.

For så vidt angår tavshedspligt for tilsynsmyndighedens medlemmer og personale henvises til afsnit 7.3. om bl.a. artikel 54, stk. 2, som videreführer databeskyttelsesdirektivets artikel 28, stk. 7, om tavshedspligt for tilsynsmyndighedens medlemmer og personale.

10.7.2. Gældende ret

Det følger af databeskyttelsesdirektivets artikel 28, stk. 3, 1. pkt., at tilsynsmyndigheden bl.a. skal kunne iværksætte undersøgelser og bl.a. have adgang til de oplysninger, der gøres til genstand for behandling, og til at indsamle alle oplysninger, der er nødvendige for at varetage dens tilsynsopgaver.

I forlængelse heraf følger det af persondatalovens § 62, stk. 1, 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.

Det følger desuden af § 62, stk. 2, at tilsynets medlemmer og personale til enhver tid mod behørig legitimation uden retskendelse har adgang til alle lokaler, hvorfra en behandling, som foretages for den offentlige forvaltning, administreres, eller hvorfra der er adgang til de oplysninger, som behandles, samt til lokaler, hvor oplysningerne eller tekniske hjælpemidler opbevares eller anvendes.

Der er således ikke fastsat særlige begrænsninger i Datatilsynets beføjelser til i medfør af persondatalovens § 62, stk. 1, at kræve oplysninger i tilfælde, hvor de oplysninger, som behandles, er underlagt tavshedspligt.

Der er heller ikke fastsat særlige begrænsninger i Datatilsynets inspektionsbeføjelser i forhold til oplysninger, som er underlagt tavshedspligt.

Datatilsynets inspektionskompetence i forhold til behandlinger, som foretages *for private* er dog, i medfør af persondatalovens § 62, stk. 3, begrænset til de typer af behandlinger, som er undergivet et krav om forudgående tilladelse, jf. persondatalovens § 50, eller behandlinger, som foretages i forbindelse med tv-overvågning.

10.7.3. Databeskyttelsesforordningen

Det fremgår af forordningens artikel 90, at medlemsstaterne kan vedtage specifikke regler om *tilsynsmyndighedernes beføjelser* i henhold til artikel 58, stk. 1, litra e, om adgang til personoplysninger og oplysninger, der er nødvendige for varetagelse for tilsynsopgaven, og litra f, om adgang til lokaler, herunder databehandlingsudstyr og -midler, vedrørende dataansvarlige eller databehandlere, der i henhold til *EU-ret* eller *medlemsstaternes natio-*

nale ret eller *regler fastsat af nationale kompetente organer* er underlagt faglig eller anden tavshedspligt, hvis dette er nødvendigt og rimeligt for at forene retten til beskyttelse af personoplysninger med tavshedspligt.

Det fremgår desuden af artikel 90, at disse regler kun gælder for *personoplysninger*, som den dataansvarlige eller databehandleren har modtaget som et resultat af eller indhentet under *en aktivitet, der er underlagt denne tavshedspligt*.

Det fremgår af præambelbetragtning nr. 164, at de specifikke regler, som kan vedtages i medfør af artikel 90, skal være inden for rammerne af databeskyttelsesforordningen. Det fremgår desuden, at dette ikke berører medlemsstaternes eksisterende forpligtelser til at vedtage regler om tavshedspligt, hvis det kræves i EU-retten.

Det, der i medfør af bestemmelsen kan fastsættes specifikke bestemmelser om, er *tilsynsmyndighedernes undersøgelsesbeføjelser* vedrørende dataansvarlige og databehandlere ved 1) adgang til alle personoplysninger og oplysninger (artikel 58, litra e), samt ved 2) adgang til alle lokaler, herunder til databehandlingsudstyr og -midler (artikel 58, litra f).

De specifikke bestemmelser om tilsynsmyndighedernes undersøgelsesbeføjelser kan alene angå *personoplysninger*, som den dataansvarlige eller databehandleren har modtaget som et resultat af eller indhentet under *en aktivitet, der er underlagt en tavshedspligt*. Modsætningsvist kan der ikke i medfør af bestemmelsen fastsættes specifikke regler om tilsynsmyndighedens kompetence i relation til personoplysninger modtaget eller indhentet i forbindelse med en aktivitet, som ikke er underlagt tavshedspligt.

Om karakteren af tavshedspligten i denne sammenhæng, fremgår det af artikel 90, at der skal være tale om en faglig eller anden tavshedspligt, som den dataansvarlige eller databehandleren er underlagt i medfør af *EU-ret, national ret* eller *regler fastsat af nationale kompetente organer*.

Det fremgår af artikel 90, stk. 2, at hver medlemsstat senest den 25. maj 2018 giver Kommissionen meddelelse om de regler, som den vedtager i henhold til stk. 1, og underretter den straks om alle senere ændringer, der berører dem.

10.7.4. Overvejelser

Muligheden for at fastsætte særlige regler om tilsynsmyndighedernes undersøgelsesbeføjelser i forhold til oplysninger, som er underlagt tavshedspligt, skal overvejes i forbindelse med de nærmere overvejelser om tilsynsmyndighedernes beføjelser i medfør af artikel 58.

Det vil under alle omstændigheder i forhold til artikel 90 være muligt at videreføre ordningen i § 62 i persondataloven, hvorefter der ikke er begrænsninger i Datatilsynets adgang til at kræve oplysninger som led i tilsynet, samtidig med, at Datatilsynets personale selv er underlagt tavshedspligt, jf. forvaltningslovens § 27 og straffelovens § 152 og §§ 152 c-f.

Endelig bemærkes, at artikel 90 forudsætter at medlemsstaterne kan opretholde og indføre nationale bestemmelser om tavshedspligt.

10.8. Rammerne i artikel 91 vedrørende kirkers og religiøse sammenslutningers eksisterende databeskyttelsesregler

10.8.1. Præsentation

Databeskyttelsesforordningens artikel 91 indeholder en særlig regel om videreførelse af eksisterende databeskyttelsesregler for kirker og religiøse sammenslutningers behandling af personoplysninger inden for rammerne af forordningen.

10.8.2. Gældende ret

I det omfang kirker og religiøse sammenslutninger behandler personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, finder persondataloven – i lighed med hvad tilfældet er for andre dataansvarlige – anvendelse, jf. persondatalovens § 1, stk. 1.

For så vidt angår kirkers behandling af personoplysninger har Datatilsynet i en udtalelse om Ribe Stifts direkte transmission af gudstjenester mv. udtalt, at det er menighedsrådene, der er ansvarlige for den behandling af personoplysninger, der finder sted i forbindelse med transmission af gudstjenester til lokale plejehjem og visning på skærme i kirken.[1005] Dermed fandt Datatilsynet bl.a., at den pågældende behandling af personoplysninger var omfattet af persondataloven.

Der er ikke i dansk ret fastsat regler om databeskyttelse for kirker og religiøse sammenslutningers behandling af personoplysninger.

10.8.3. Databeskyttelsesforordningen

Det fremgår af forordningens præambelbetragtning nr. 165, at forordningen respekterer og ikke anfægter den status i henhold til eksisterende forfatningsretlige bestemmelser, som kirker og religiøse sammenslutninger eller samfund har i medlemsstaterne, jf. artikel 17 i TEUF.

[1005] Datatilsynets j.nr. 2012-218-0006, gengivet i Persondataloven med kommentarer (2015), s. 243.

Det fremgår endvidere af forordningen artikel 91, stk. 1, at hvis kirker og religiøse sammenslutninger eller samfund i en medlemsstat på tidspunktet for forordningens ikrafttrædelse anvender omfattende regler om beskyttelse af fysiske personer hvad angår behandling, kan disse eksisterende regler fortsat finde anvendelse, forudsat at de bringes i overensstemmelse med forordningen.

Det fremgår endvidere af artikel 91, stk. 2, at kirker og religiøse sammenslutninger, der anvender omfattende regler i henhold til bestemmelsens stk. 1, underlægges tilsyn af en uafhængig tilsynsmyndighed, som kan være specifik, forudsat at den opfylder betingelserne i kapitel VI i forordningen om uafhængige tilsynsmyndigheder.

10.8.4. Overvejelser

Idet, der i dag ikke i dansk ret er fastsat regler om databeskyttelse for kirker og religiøse sammenslutningers behandling af personoplysninger, forventes forordningens artikel 91 ikke at få betydning for den danske databeskyttelseslovgivning.

11. Forordningens kapitel X og XI: Delegerede retsakter, gennemførelsesbestemmelser og afsluttende bestemmelser

11.1. Forordningens kapitel X og XI om afsluttende bestemmelser (artikel 92-99)

11.1.1. Kommissionens delegerede beføjelser, artikel 92

Det følger af forordningens artikel 92, stk. 1, at Kommissionen er tillagt beføjelse til at vedtage *delegerede retsakter* under de betingelser, der følger af de øvrige stykker i artikel 92.

Det fremgår af forordningens præambelbetragtning nr. 166, 1. pkt., at beføjelsen til at vedtage retsakter i henhold til artikel 290 i TEUF delegeres til Kommissionen for at opfylde forordningens målsætninger, dvs. at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger, og for at sikre fri udveksling af personoplysninger i Unionen.

Ifølge forordningens artikel 92, stk. 2, har Kommissionen fra den 24. maj 2016 i en ubegrænset periode beføjelse til at vedtage delegerede retsakter i medfør af forordningens artikel 12, stk. 8, om standardiserede ikoner i oplysninger, der gives til den registrerede, og i medfør af artikel 43, stk. 8, om krav til certificeringsmekanismer for databeskyttelse.

Herom fremgår det af forordningens præambelbetragtning nr. 166, 2. pkt., at der navnlig bør vedtages delegerede retsakter om kriterier for og krav til certificeringsmekanismer. Endvidere bør der navnlig vedtages delegerede retsakter om oplysninger, der skal fremgå af standardiserede ikoner, og procedurer for tilvejebringelse af sådanne ikoner.

Det følger af forordningens artikel 92, stk. 3, at Europa-Parlamentet og Rådet til enhver tid kan tilbagekalde delegationen som fastsat i artikel 12, stk. 8, og artikel 43, stk. 8. En sådan afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

Efter forordningens artikel 92, stk. 4, skal Kommissionen give Europa-Parlamentet og Rådet meddelelse om en delegeret retsakt samtidig med vedtagelsen af retsakten.

Ifølge artikel 92, stk. 5, træder en delegeret retsakt vedtaget i henhold til artikel 12, stk. 8, og artikel 43, stk. 8, kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på tre måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet eller Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Fristen kan forlænges med tre måneder på Europa- Parlamentets eller Rådets initiativ.

Supplerende følger det af forordningens præambelbetragtning nr. 166, 3. pkt., at det navnlig er vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at Kommissionen bør sikre samtidig, rettidig og hensigtsmæssig fremsendelse af relevante dokumenter til Europa-Parlamentet og til Rådet, når den forbereder og udarbejder delegerede retsakter.

11.1.2. Bistand fra udvalg ved Kommissionens vedtagelse af gennemførelsesretsakter, artikel 93

Kommissionen er tillagt gennemførelsesbeføjelser i forordningens artikel 40, stk. 9, om generel gyldighed af adfærdskodekser, artikel 43, stk. 9, om tekniske standarder for certificeringsmekanismer mv., artikel 45, stk. 3 og 5, om tilstrækkelighed af beskyttelsesniveau i tredjelande, artikel 47, stk. 3, om format og procedurer for bindende virksomhedsregler, artikel 61, stk. 9, om format og procedurer for gensidig bistand mellem tilsynsmyndigheder mv. samt artikel 67 om ordninger for elektronisk udveksling af oplysninger mellem tilsynsmyndigheder mv.

I forbindelse med udøvelsen af disse beføjelser skal Kommissionen ifølge forordningens artikel 93, stk. 1, bistås af et udvalg omhandlet i forordning (EU) nr. 182/2011.

Herom følger det af databeskyttelsesforordningens præambelbetragtning nr. 167, at Kommissionen bør tillægges *gennemførelsesbeføjelser* for at sikre ensartede betingelser for gennemførelsen af forordningen, når dette er fastsat i forordningen, og at disse gennemførelsesbeføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011.

Forordning (EU) nr. 182/2011 fastsætter de generelle regler og principper for de mekanismer, der finder anvendelse, når det i en retligt bindende EU-retsakt (herefter »basisretsakt«) fastsættes, at ensartede betingelser for gennemførelse er nødvendige, og kræves, at Kommissionens vedtagelse af gennemførelsesretsakter skal kontrolleres af medlemsstaterne, jf. denne forordnings artikel 1. Udvalget er ifølge artikel 3, stk. 2, i forordning (EU) nr. 182/2011 sammensat af repræsentanter for medlemsstaterne. Ifølge denne bestemmelse er

det er en repræsentant for Kommissionen, som varetager udvalgets formandskab, men formanden deltager ikke i udvalgets afstemninger.

Ifølge databeskyttelsesforordningens artikel 93, stk. 2, finder artikel 5 om udvalgsproceduren i forordning (EU) nr. 182/2011 anvendelse, når der henvises til dette stykke, jf. herved også præambelbetragtning nr. 168. Det kan hertil bemærkes, at det følger af ovennævnte beføjelsesbestemmelser, at disse gennemførelsesforanstaltninger mv. vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

Efter databeskyttelsesforordningens artikel 93, stk. 3, finder hasteproceduren i forordning (EU) nr. 182/2011, artikel 8 sammenholdt med artikel 5, anvendelse, når der henvises til artikel 93, stk. 3.

Herom følger det af databeskyttelsesforordningens præambelbetragtning nr. 169, at Kommissionen bør vedtage gennemførelsesretsakter, der finder anvendelse straks, når foreliggende dokumentation viser, at et tredjeland, et område eller en specifik sektor i dette tredjeland, eller en international organisation ikke sikrer et tilstrækkeligt beskyttelsesniveau, og når det er påkrævet i særlig hastende tilfælde.

11.1.3. Ophævelse af databeskyttelsesdirektivet (direktiv 95/46/EF), artikel 94

Det følger af databeskyttelsesforordningens artikel 94, at databeskyttelsesdirektivet ophæves med virkning fra den 25. maj 2018, det vil sige samtidig med tidspunktet, hvorfra forordningen finder anvendelse, jf. artikel 99.

Endvidere følger det af artikel 94, at henvisninger til det ophævede direktiv fra den 25. maj 2018 gælder som henvisninger til forordningen, og at henvisninger til Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved artikel 29 i databeskyttelsesdirektivet (Artikel 29-gruppen), gælder som henvisninger til Det Europæiske Databeskyttelsesråd oprettet ved forordningen.

11.1.4. Forholdet til direktiv 2002/58/EF om offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet, artikel 95

Ifølge forordningens artikel 95 indfører forordningen ikke yderligere forpligtelser for fysiske eller juridiske personer for så vidt angår behandling i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet i Unionen for så vidt angår spørgsmål, hvor de er underlagt specifikke forpligtelser med samme formål som det, der er fastsat i direktiv 2002/58/EF.

11.1.5. Forholdet til allerede indgåede internationale aftaler om overførsel af personoplysninger til tredjelande mv., artikel 96

Det følger af forordningens artikel 96, at internationale aftaler, der omfatter overførsel af personoplysninger til tredjelande eller internationale organisationer, som er indgået af medlemsstaterne inden den 24. maj 2016, og som overholder den EU-ret, der finder anvendelse inden denne dato, forbliver i kraft, indtil de ændres, erstattes eller ophæves.

11.1.6. Evaluering og revision af forordningen, artikel 97

I forordningens artikel 97, stk. 1, er det fastsat, at Kommissionen senest den 25. maj 2020 og hvert fjerde år derefter forelægger Europa-Parlamentet og Rådet en rapport om evaluering og revision af forordningen.

Ifølge artikel 97, stk. 2, skal Kommissionen i den forbindelse navnlig undersøge, hvordan kapitel V om overførsel af personoplysninger til tredjelande eller internationale organisationer anvendes og fungerer, særligt med hensyn til afgørelser vedtaget i henhold til denne forordnings artikel 45, stk. 3, og afgørelser vedtaget på grundlag af artikel 25, stk. 6, i databeskyttelsesdirektivet. Endvidere følger det af artikel 97, stk. 2, at Kommissionen i den forbindelse navnlig skal undersøge, hvordan kapitel VII om samarbejde og sammenhæng anvendes og fungerer.

Endvidere følger det af artikel 97, stk. 3, at Kommissionen med henblik på evaluering og revision som omhandlet i artikel 97, stk. 1, kan anmode om oplysninger fra medlemsstaterne og tilsynsmyndighederne.

Desuden følger det af artikel 97, stk. 4, at Kommissionen tager hensyn til holdninger og resultater fra Europa-Parlamentet, fra Rådet og fra andre relevante organer eller kilder, når Kommissionen foretager evaluering og revision som omhandlet i artikel 97, stk. 1 og 2.

Endelig følger det af artikel 97, stk. 5, at Kommissionen om nødvendigt forelægger relevante forslag til ændring af forordningen, og at sådanne forslag navnlig skal forelægges under hensyntagen til udviklingen inden for informationsteknologi og i lyset af fremskridtene i informationssamfundet.

11.1.7. Relevante ændringer af andre EU-retsakter, artikel 98

Det følger af forordningens artikel 98, at Kommissionen fremsætter lovgivningsforslag til ændring af andre EU-retsakter om beskyttelse af personoplysninger, hvis det er relevant, for at sikre ensartet og konsekvent beskyttelse af fysiske personer i forbindelse med behandling. Endvidere følger det heraf, at dette især gælder bestemmelser om beskyttelse af

fysiske personer i forbindelse med EU-institutioners, -organers, -kontorers og -agenturers behandling og om fri udveksling af sådanne oplysninger.

11.1.8. Ikrafttrædelse, anvendelse og virkning, artikel 99

Efter forordningens artikel 99, stk. 1, træder forordningen i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Efter forordningens artikel 99, stk. 2, 1. pkt., skal forordningen anvendes fra den 25. maj 2018.

I forordningens artikel 99, stk. 2, 2. pkt., understreges forordningens horisontale virkning efter artikel 288, 2. pkt., i TEUF, hvorefter forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

I

(Lovgivningsmæssige retsakter)

FORORDNINGER

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679

af 27. april 2016

om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ([1]),

under henvisning til udtalelse fra Regionsudvalget ([2]),

efter den almindelige lovgivningsprocedure ([3]), og

ud fra følgende betragtninger:

(1) Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger er en grundlæggende rettighed. I artikel 8, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder (»chartret«) og i artikel 16, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde (TEUF) fastsættes det, at enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.

(2) Principperne og reglerne for beskyttelse af fysiske personer i forbindelse med behandling af deres personoplysninger bør, uanset deres nationalitet eller bopæl, respektere deres grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger. Denne forordning har til formål at bidrage til skabelsen af et område med frihed, sikkerhed og retfærdighed samt en økonomisk union og til økonomiske og sociale fremskridt, styrkelse af og konvergens mellem økonomierne inden for det indre marked og fysiske personers velfærd.

(3) Europa-Parlamentets og Rådets direktiv 95/46/EF ([4]) har til formål at harmonisere beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandlingsaktiviteter og at sikre den frie udveksling af personoplysninger mellem medlemsstaterne.

([1]) EUT C 229 af 31.7.2012, s. 90.
([2]) EUT C 391 af 18.12.2012, s. 127.
([3]) Europa-Parlamentets holdning af 12.3.2014 (endnu ikke offentliggjort i EUT) og Rådets førstebehandlingsholdning af 8.4.2016 (endnu ikke offentliggjort i EUT). Europa-Parlamentets holdning af 14.4.2016.
([4]) 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 (EFT L 281 af 23.11.1995, s. 31).

(4) Behandling af personoplysninger bør have til formål at tjene menneskeheden. Retten til beskyttelse af personoplysninger er ikke en absolut ret; den skal ses i sammenhæng med sin funktion i samfundet og afvejes i forhold til andre grundlæggende rettigheder i overensstemmelse med proportionalitetsprincippet. Denne forordning overholder alle de grundlæggende rettigheder og følger de frihedsrettigheder og principper, der anerkendes i chartret som forankret i traktaterne, navnlig respekten for privatliv og familieliv, hjem og kommunikation, beskyttelsen af personoplysninger, retten til at tænke frit, til samvittigheds- og religionsfrihed, ytrings- og informationsfrihed, frihed til at oprette og drive egen virksomhed, adgang til effektive retsmidler og til en retfærdig rettergang og kulturel, religiøs og sproglig mangfoldighed.

(5) Den økonomiske og sociale integration, der er en følge af det indre markeds funktion, har medført en kraftig vækst i bevægelserne af personoplysninger på tværs af landegrænserne. Udvekslingen af personoplysninger mellem offentlige og private aktører, herunder fysiske personer, sammenslutninger og virksomheder, i Unionen er steget. De nationale myndigheder i medlemsstaterne opfordres i EU-retten til at samarbejde og udveksle personoplysninger for at kunne varetage deres hverv og udføre opgaver på vegne af en myndighed i en anden medlemsstat.

(6) Den hastige teknologiske udvikling og globaliseringen har skabt nye udfordringer, hvad angår beskyttelsen af personoplysninger. Omfanget af indsamlingen og delingen af personoplysninger er steget betydeligt. Teknologien giver både private selskaber og offentlige myndigheder mulighed for at udnytte personoplysninger i et hidtil uset omfang, når de udøver deres aktiviteter. Fysiske personer udbreder i stigende grad deres personoplysninger offentligt og globalt. Teknologien har ændret både økonomien og sociale aktiviteter og bør yderligere fremme den frie udveksling af personoplysninger inden for Unionen og overførslen af oplysninger til tredjelande og internationale organisationer, samtidig med at der sikres et højt niveau for beskyttelse af personoplysninger.

(7) Denne udvikling kræver en stærk og mere sammenhængende databeskyttelsesramme i Unionen, som understøttes af effektiv håndhævelse, fordi det er vigtigt at skabe den tillid, der gør det muligt, at den digitale økonomi kan udvikle sig på det indre marked. Fysiske personer bør have kontrol over deres personoplysninger. Sikkerheden både retligt og praktisk bør styrkes for fysiske personer, erhvervsdrivende og offentlige myndigheder.

(8) Når denne forordning 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.

(9) Målsætningerne og principperne i direktiv 95/46/EF er stadig gyldige, men direktivet har ikke forhindret en fragmentering af gennemførelsen af databeskyttelse i Unionen, manglende retssikkerhed eller en udbredt offentlig opfattelse af, at der er betydelige risici for beskyttelsen af fysiske personer, navnlig i forbindelse med onlineaktivitet. Forskelle i niveauet for beskyttelsen af fysiske personers rettigheder og frihedsrettigheder, navnlig retten til beskyttelse af personoplysninger, i forbindelse med behandling af personoplysninger i medlemsstaterne, kan forhindre fri udveksling af personoplysninger i Unionen. Disse forskelle kan derfor udgøre en hindring for udøvelsen af en række økonomiske aktiviteter på EU-plan, virke konkurrenceforvridende og hindre myndighederne i at varetage de opgaver, de er pålagt i medfør af EU-retten. En sådan forskel i beskyttelsesniveauet skyldes forskelle i gennemførelsen og anvendelsen af direktiv 95/46/EF.

(10) 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. 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. Sammen med generel og horisontal lovgivning om databeskyttelse til gennemførelse af direktiv 95/46/EF har medlemsstaterne flere sektorspecifikke love på områder, hvor der er behov for mere specifikke bestemmelser. Denne forordning indeholder også en manøvremargen, så medlemsstaterne kan præcisere reglerne heri, herunder for behandling af særlige kategorier af personoplysninger (»følsomme oplysninger«). Denne forordning udelukker således ikke, at medlemsstaternes nationale ret fastlægger omstændighederne i forbindelse med specifikke databehandlingssituationer, herunder mere præcis fastlæggelse af de forhold, hvorunder behandling af personoplysninger er lovlig.

(11) For at sikre effektiv beskyttelse af personoplysninger i Unionen er det nødvendigt at styrke og præcisere de registreredes rettigheder og de forpligtelser, der påhviler dem, der behandler og træffer afgørelse om behandling af personoplysninger, samt at der gives tilsvarende beføjelser til at føre tilsyn med og sikre overholdelse af reglerne om beskyttelse af personoplysninger og indføres tilsvarende sanktioner ved overtrædelser i medlemsstaterne.

(12) Artikel 16, stk. 2, i TEUF giver Europa-Parlamentet og Rådet beføjelse til at fastsætte regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og regler om fri udveksling af sådanne oplysninger.

(13) For at sikre et ensartet beskyttelsesniveau for fysiske personer i hele Unionen 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. Et velfungerende indre marked kræver, 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. For at tage hensyn til den særlige situation for mikrovirksomheder og små og mellemstore virksomheder indeholder denne forordning en undtagelse for organisationer med mindre end 250 ansatte med hensyn til at føre fortegnelser. Derudover opfordres EU-institutionerne og -organerne samt medlemsstaterne og deres tilsynsmyndigheder til at tage hensyn til mikrovirksomheders og små og mellemstore virksomheders særlige behov i forbindelse med anvendelsen af denne forordning. Begreberne mikrovirksomheder og små og mellemstore virksomheder bør baseres på artikel 2 i bilaget til Kommissionens henstilling 2003/361/EF ([1]).

(14) Den beskyttelse, som denne forordning yder i forbindelse med behandling af personoplysninger, bør finde anvendelse på fysiske personer uanset nationalitet eller bopæl. Denne forordning finder ikke anvendelse på behandling af personoplysninger, der vedrører juridiske personer, navnlig virksomheder, der er etableret som juridiske personer, herunder den juridiske persons navn, form og kontaktoplysninger.

(15) For at undgå at skabe en alvorlig risiko for omgåelse bør beskyttelsen af fysiske personer være teknologineutral og ikke afhænge af de anvendte teknikker. 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. Sagsmapper eller samlinger af sagsmapper samt deres forsider, som ikke er struktureret efter bestemte kriterier, bør ikke være omfattet af denne forordnings anvendelsesområde.

(16) Denne forordning finder ikke 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. Denne forordning finder ikke anvendelse på behandling af personoplysninger, der foretages af medlemsstaterne, når de udfører aktiviteter i forbindelse med Unionens fælles udenrigs- og sikkerhedspolitik.

(17) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 ([2]) finder anvendelse på behandling af personoplysninger, der foretages af Unionens institutioner, organer, kontorer og agenturer. Forordning (EF) nr. 45/2001 og andre EU-retsakter, der finder anvendelse på sådan behandling af personoplysninger, bør tilpasses til principperne og bestemmelserne fastsat i nærværende forordning og anvendes i lyset af nærværende forordning. Med henblik på at sikre en stærk og sammenhængende databeskyttelsesramme i Unionen bør de nødvendige tilpasninger af forordning (EF) nr. 45/2001 følge efter vedtagelsen af nærværende forordning, således at de finder anvendelse samtidig med nærværende forordning.

(18) Denne forordning gælder ikke 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

([1]) Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (C(2003) 1422) (EUT L 124 af 20.5.2003, s. 36).

([2]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001, s. 1).

eller familiemæssige aktiviteter kan omfatte korrespondance og føring af en adressefortegnelse eller sociale netværksaktiviteter og onlineaktiviteter, der udøves som led i sådanne aktiviteter. Denne forordning gælder dog for dataansvarlige eller databehandlere, som tilvejebringer midlerne til behandling af personoplysninger til sådanne personlige eller familiemæssige aktiviteter.

(19) Beskyttelse af fysiske personer i forbindelse med de kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskyttelsen mod og forebyggelsen af trusler mod den offentlige sikkerhed og den frie udveksling af sådanne oplysninger, er genstand for en specifik EU-retsakt. Denne forordning bør derfor ikke gælde for behandlingsaktiviteter med disse formål. Behandling af personoplysninger af offentlige myndigheder, som er omfattet af denne forordning, med henblik på disse formål bør imidlertid være genstand for en mere specifik EU-retsakt, Europa-Parlamentets og Rådets direktiv (EU) 2016/680 ([1]). 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 direktiv (EU) 2016/680, således at behandling af personoplysninger til disse andre formål, for så vidt som de er omfattet af EU-retten, falder ind under denne forordnings anvendelsesområde.

Med hensyn til disse kompetente myndigheders behandling af personoplysninger til formål, der er omfattet af anvendelsesområdet for denne forordning, bør medlemsstaterne 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 denne forordnings 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.

(20) Selv om denne forordning bl.a. finder anvendelse på domstoles og andre judicielle myndigheders aktiviteter, kan EU-retten eller medlemsstaternes nationale ret præcisere, hvilke behandlingsaktiviteter og -procedurer der finder anvendelse i forbindelse med domstoles og andre judicielle myndigheders behandling af personoplysninger. Tilsynsmyndighedernes kompetence bør af hensyn til dommerstandens uafhængighed under udførelsen af dens judicielle opgaver, herunder ved beslutningstagning, ikke omfatte domstolenes behandling af personoplysninger, når domstole handler i deres egenskab af domstol. Tilsynet med sådanne databehandlingsaktiviteter bør kunne overdrages til specifikke organer i medlemsstatens retssystem, der navnlig bør sikre overholdelsen af reglerne i denne forordning, gøre dommerstanden bekendt med dens forpligtelser i henhold til denne forordning og behandle klager over sådanne databehandlingsaktiviteter.

(21) Denne forordning berører ikke anvendelsen af Europa-Parlamentets og Rådets direktiv 2000/31/EF ([2]), navnlig reglerne om formidleransvar for tjenesteydere, der er fastsat i artikel 12-15 i dette direktiv. Direktivet har til formål at bidrage til et velfungerende indre marked ved at sikre den frie bevægelighed for informationssamfundstjenester mellem medlemsstaterne.

(22) Enhver behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i Unionen, bør gennemføres i overensstemmelse med denne forordning, uanset om selve behandlingen finder sted i Unionen. Etablering indebærer effektiv og faktisk udøvelse af aktivitet gennem en mere permanent struktur. De pågældende ordningers retlige form, hvad enten det er en filial eller et datterselskab med status som juridisk person, har ikke afgørende betydning i denne forbindelse.

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (se side 89 i denne EUT).

([2]) Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (»Direktivet om elektronisk handel«) (EFT L 178 af 17.7.2000, s. 1).

(23) For at sikre, at fysiske personer ikke unddrages den beskyttelse, som de har ret til i medfør af denne forordning, bør behandling af personoplysninger om registrerede, der er i Unionen, som foretages af en dataansvarlig eller en databehandler, der ikke er etableret i Unionen, være omfattet af denne forordning, hvis behandlingsaktiviteterne vedrører udbud af varer eller tjenesteydelser til sådanne registrerede, uanset om de er knyttet til en betaling. Med henblik på at afgøre, om en sådan dataansvarlig eller databehandler udbyder varer eller tjenesteydelser til registrerede, der befinder sig i Unionen, bør det undersøges, om det er åbenbart, at den dataansvarlige eller databehandleren påtænker at udbyde tjenesteydelser til registrerede i en eller flere EU-medlemsstater. Selv om det forhold, at der er adgang til den dataansvarliges, databehandlerens eller en mellemmands websted i Unionen, til en e-mailadresse eller til andre kontaktoplysninger, eller at der anvendes et sprog, der almindeligvis anvendes i det tredjeland, hvor den dataansvarlige er etableret, i sig selv er utilstrækkeligt til at fastslå en sådan hensigt, kan faktorer såsom anvendelse af et sprog eller en valuta, der almindeligvis anvendes i en eller flere medlemsstater, med mulighed for at bestille varer og tjenesteydelser på det pågældende sprog eller omtale af kunder eller brugere, der befinder sig i Unionen, gøre det åbenbart, at den dataansvarlige påtænker at udbyde varer eller tjenesteydelser til registrerede i Unionen.

(24) Behandling af personoplysninger om registrerede, der befinder sig i Unionen, foretaget af en dataansvarlig eller en databehandler, der ikke er etableret i Unionen, bør også være omfattet af denne forordning, når den vedrører overvågning af sådanne registreredes adfærd, så længe denne adfærd foregår inden for Unionen. 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.

(25) Hvis medlemsstaternes nationale ret finder anvendelse i medfør af folkeretten, bør denne forordning også gælde for en dataansvarlig, der ikke er etableret i Unionen, som f.eks. ved en medlemsstats diplomatiske eller konsulære repræsentation.

(26) Principperne for databeskyttelse bør gælde for enhver information om en identificeret eller identificerbar fysisk person. 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. 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. 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. Databeskyttelsesprincipperne bør derfor ikke 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. Denne forordning vedrører derfor ikke behandling af sådanne anonyme oplysninger, herunder til statistiske eller forskningsmæssige formål.

(27) Denne forordning finder ikke anvendelse på personoplysninger om afdøde personer. Medlemsstaterne kan fastsætte regler for behandling af personoplysninger om afdøde personer.

(28) Anvendelsen af pseudonymisering af personoplysninger kan mindske risikoen for de berørte registrerede og gøre det lettere for dataansvarlige og databehandlere at opfylde deres databeskyttelsesforpligtelser. Det er ikke tanken med den udtrykkelige indførelse af »pseudonymisering« i denne forordning at udelukke andre databeskyttelsesforanstaltninger.

(29) For at skabe incitamenter til anvendelse af pseudonymisering i forbindelse med behandling af personoplysninger bør pseudonymiseringsforanstaltninger, som samtidig tillader en generel analyse, under den samme dataansvarlige være mulige, når den dataansvarlige har truffet de tekniske og organisatoriske foranstaltninger, der er nødvendige for at sikre, at denne forordning gennemføres for så vidt angår den pågældende behandling, og at yderligere oplysninger, der gør det muligt at henføre personoplysninger til en bestemt registreret, opbevares separat. Den dataansvarlige, som behandler personoplysningerne, bør anføre de autoriserede personer under den samme dataansvarlige.

(30) Fysiske personer kan tilknyttes onlineidentifikatorer, som tilvejebringes af deres enheder, applikationer, værktøjer og protokoller, såsom IP-adresser og cookieidentifikatorer, eller andre identifikatorer, såsom radiofrekvensidentifikationsmærker. 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.

(31) Offentlige myndigheder, til hvem personoplysninger videregives i overensstemmelse med en retlig forpligtelse i forbindelse med udøvelsen af deres officielle hverv, såsom skatte- og toldmyndigheder, finansielle efterforskningsenheder, uafhængige administrative myndigheder eller finansielle markedsmyndigheder, der er ansvarlige for regulering af og tilsyn med værdipapirmarkederne, bør ikke betragtes som værende modtagere, hvis de modtager personoplysninger, der er nødvendige som led i en isoleret forespørgsel af almen interesse i overensstemmelse med EU-retten eller medlemsstaternes nationale ret. Anmodninger om videregivelse af oplysninger sendt af offentlige myndigheder bør altid være skriftlige, begrundede og lejlighedsvise og bør ikke vedrøre et register som helhed eller føre til samkøring af registre. Disse offentlige myndigheders behandling af personoplysninger bør være i overensstemmelse med de gældende databeskyttelsesregler afhængigt af formålet med behandlingen.

(32) 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.

(33) Det er ofte ikke 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.

(34) 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.

(35) 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 ([1]), 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.

(36) En dataansvarligs 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

([1]) Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).

anses for at være hovedvirksomheden. 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. Dette kriterium bør ikke afhænge af, om behandling af personoplysninger foretages på dette sted. Det forhold, at der findes og anvendes tekniske midler og teknologi til behandling af personoplysninger eller behandlingsaktiviteter, medfører ikke i sig selv, at der er etableret en hovedvirksomhed, og er derfor ikke afgørende for kriteriet om hovedvirksomhed. 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. 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. Foretages behandlingen af en koncern, bør den kontrollerende virksomheds hovedvirksomhed anses for at være koncernens hovedvirksomhed, medmindre formål og hjælpemidler fastlægges af en anden virksomhed.

(37) 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. En virksomhed, der udøver kontrol med behandlingen af personoplysninger i de virksomheder, der er knyttet til den, bør sammen med disse virksomheder anses som en koncern.

(38) 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. Samtykke fra indehaveren af forældremyndigheden er ikke nødvendigt, når det drejer sig om forebyggende eller rådgivende tjenester, der tilbydes direkte til et barn.

(39) 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. Især bør de specifikke formål med behandlingen af personoplysninger være udtrykkelige og legitime og fastlagt, når personoplysningerne indsamles. 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. For at sikre, at personoplysninger ikke opbevares i længere tid end nødvendigt, bør den dataansvarlige indføre tidsfrister for sletning eller periodisk gennemgang. Der bør træffes enhver rimelig foranstaltning for at sikre, at personoplysninger, som er urigtige, berigtiges eller slettes. 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.

(40) 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.

(41) 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. 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 Den Europæiske Unions Domstol (»Domstolen«) og Den Europæiske Menneskerettighedsdomstol.

(42) Hvis behandling er baseret på den registreredes samtykke, bør den dataansvarlige kunne påvise, at den registrerede har givet samtykke til behandlingen. 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 ([1]) 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. Samtykke bør ikke 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.

(43) 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. 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.

(44) Behandling bør anses for lovlig, når den er nødvendig i forbindelse med en kontrakt eller en påtænkt indgåelse af en kontrakt.

(45) 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. Det bør ligeledes 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.

(46) Behandling af personoplysninger, der er nødvendig for at beskytte et hensyn af fundamental betydning for den registreredes eller en anden fysisk persons liv, bør ligeledes anses for lovlig. Behandling af personoplysninger på

([1]) Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår i forbrugeraftaler (EFT L 95 af 21.4.1993, s. 29).

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.

(47) 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 interesser, hvis personoplysninger behandles under omstændigheder, hvor registrerede ikke med rimelighed forventer viderebehandling. 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. 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.

(48) Dataansvarlige, der indgår i en koncern eller 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.

(49) 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.

(50) Behandling af personoplysninger til andre formål end de formål, som personoplysningerne oprindelig blev indsamlet til, bør kun tillades, hvis behandlingen er forenelig med de formål, som personoplysningerne oprindelig blev indsamlet til. I dette tilfælde kræves der ikke andet retsgrundlag end det, der begrundede indsamlingen af personoplysningerne. Hvis behandling er nødvendig for at udføre en opgave i samfundets interesse eller henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, kan EU-retten eller medlemsstaternes nationale ret fastsætte og præcisere de opgaver og formål, hvortil det bør være foreneligt og lovligt at foretage viderebehandling. Viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål bør anses for at være forenelige lovlige behandlingsaktiviteter. Retsgrundlaget i EU-retten eller medlemsstaternes nationale ret for behandling af personoplysninger kan også udgøre et retsgrundlag for viderebehandling. For at fastslå, om et formål med viderebehandling er foreneligt med det formål, som personoplysningerne oprindelig blev indsamlet til, bør den dataansvarlige efter at have opfyldt alle kravene til lovlighed af den oprindelige behandling bl.a. tage hensyn til enhver forbindelse mellem disse formål og formålet med den påtænkte viderebehandling, den sammenhæng, som personoplysningerne er blevet indsamlet i, navnlig de registreredes rimelige forventninger til den videre anvendelse heraf på grundlag af deres

forhold til den dataansvarlige, personoplysningernes art, konsekvenserne af den påtænkte viderebehandling for de registrerede og tilstedeværelse af fornødne garantier i forbindelse med både de oprindelige og de påtænkte yderligere behandlingsaktiviteter.

Når den registrerede har givet samtykke, eller 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. Under alle omstændigheder bør de principper, der fastsættes i denne forordning, og navnlig information til den registrerede om disse andre formål og om vedkommendes rettigheder, herunder retten til at gøre indsigelse, sikres. Hvis den dataansvarlige påviser mulige strafbare handlinger eller trusler mod den offentlige sikkerhed og videresender de relevante personoplysninger i enkelte eller flere sager, der vedrører den samme strafbare handling eller trusler mod den offentlige sikkerhed, til en kompetent myndighed, bør det anses som værende i den dataansvarliges legitime interesse. En sådan videresendelse i den dataansvarliges legitime interesse eller viderebehandling af personoplysninger bør forbydes, hvis behandlingen krænker en retlig eller anden bindende tavshedspligt.

(51) 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. 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. Behandling af fotografier bør ikke systematisk 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. Sådanne personoplysninger bør ikke 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.

(52) Der 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, 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. 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. En fravigelse bør desuden 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.

(53) Særlige kategorier af personoplysninger, som bør nyde højere beskyttelse, bør kun 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. Denne forordning bør derfor 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.

EU-retten eller medlemsstaternes nationale ret bør omfatte specifikke og passende foranstaltninger til at beskytte fysiske personers grundlæggende rettigheder og personoplysninger. 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.

(54) 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 ([1]), 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.

(55) Offentlige myndigheders behandling af personoplysninger med henblik på at forfølge officielt anerkendte religiøse sammenslutningers målsætninger, der er fastsat ved forfatningsretten eller ved folkeretten, foretages også i samfundets interesse.

(56) 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.

(57) Hvis de personoplysninger, der behandles af en dataansvarlig, ikke sætter den dataansvarlige i stand til at identificere en fysisk person, bør den dataansvarlige ikke være forpligtet til at indhente yderligere oplysninger for at identificere den registrerede udelukkende med det formål at overholde bestemmelserne i denne forordning. Den dataansvarlige bør dog ikke nægte at tage imod yderligere oplysninger fra den registrerede, som han eller hun giver med henblik på udøvelsen af sine rettigheder. Identifikation bør omfatte digital identifikation af en registreret, for eksempel gennem en autentifikationsmekanisme, såsom de samme legitimationsoplysninger, som den registrerede anvender til at logge på den onlinetjeneste, der tilbydes af den dataansvarlige.

(58) Princippet om gennemsigtighed kræver, at enhver oplysning, som er rettet til offentligheden eller den registrerede, er kortfattet, lettilgængelig og letforståelig, og at der benyttes et klart og enkelt sprog og endvidere, hvis det er passende, visualisering. Sådanne oplysninger kan gøres tilgængelige i elektronisk form, f.eks. når de er rettet mod offentligheden, via et websted. Dette er især relevant i situationer, hvor den hastige vækst i antallet af aktører og den anvendte teknologis kompleksitet gør det vanskeligt for den registrerede at vide og forstå, om, af hvem og til hvilket formål der indsamles personoplysninger om vedkommende, såsom i forbindelse med annoncering på internettet. Eftersom børn bør nyde særlig beskyttelse, bør alle oplysninger og meddelelser, hvis behandling er rettet mod et barn, være i et så klart og enkelt sprog, at et barn let kan forstå dem.

(59) 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. Den dataansvarlige bør også give mulighed for elektroniske anmodninger, navnlig hvis personoplysninger behandles elektronisk. Den dataansvarlige bør være forpligtet til at besvare sådanne anmodninger fra en registreret uden unødig forsinkelse og senest inden for en måned og begrunde det, hvis vedkommende ikke agter at imødekomme sådanne anmodninger.

([1]) Europa-Parlamentets og Rådets forordning (EF) nr. 1338/2008 af 16. december 2008 om fællesskabsstatistikker over folkesundhed og arbejdsmiljø (EUT L 354 af 31.12.2008, s. 70).

(60) Principperne om rimelig og gennemsigtig behandling kræver, at den registrerede informeres om behandlingsaktiviteters eksistens og deres formål. 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. Den registrerede bør desuden informeres om tilstedeværelse af profilering og konsekvenserne heraf. Hvis personoplysninger indsamles fra den registrerede, bør den registrerede også informeres om, hvorvidt den pågældende er forpligtet til at meddele personoplysningerne, og om konsekvenserne, hvis vedkommende ikke meddeler sådanne oplysninger. 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.

(61) Oplysninger om behandling af personoplysninger bør gives til den registrerede på tidspunktet for indsamlingen fra den registrerede, eller hvis personoplysningerne indhentes fra en anden kilde, inden for en rimelig periode afhængigt af de konkrete omstændigheder. Hvis personoplysninger lovligt kan videregives til en anden modtager, bør den registrerede informeres, når personoplysningerne første gang videregives til modtageren. Hvis den dataansvarlige agter at behandle personoplysningerne til et andet formål end det, hvortil de er indsamlet, bør den dataansvarlige forud for denne viderebehandling give den registrerede oplysninger om dette andet formål og andre nødvendige oplysninger. Hvis den registrerede ikke kan informeres om personoplysningernes oprindelse, fordi der er anvendt forskellige kilder, bør der gives generelle oplysninger.

(62) Det er imidlertid ikke nødvendigt at pålægge forpligtelsen til at give information, hvis den registrerede allerede er bekendt med oplysningerne, hvis registrering eller videregivelse af personoplysningerne udtrykkelig er fastsat ved lov, eller hvis det viser sig at være umuligt eller vil kræve en uforholdsmæssigt stor indsats at underrette den registrerede. Sidstnævnte kan navnlig være tilfældet i forbindelse med behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål. I denne forbindelse bør der tages hensyn til antallet af registrerede, oplysningernes alder og eventuelle fornødne garantier, der er stillet.

(63) 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. Enhver registreret bør derfor 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. Denne ret bør ikke 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.

(64) 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. En dataansvarlig bør ikke opbevare personoplysninger alene for at kunne reagere på mulige anmodninger.

(65) 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. En registreret bør navnlig have ret til at få sine personoplysninger slettet og ikke længere behandlet, hvis personoplysningerne ikke længere er nødvendige til de formål, hvortil de er blevet indsamlet eller på anden måde behandlet, hvis en registreret har trukket sit samtykke tilbage eller gør indsigelse mod behandling af personoplysninger om vedkommende, eller hvis behandlingen af vedkommendes personoplysninger i øvrigt ikke er i overensstemmelse med denne forordning. Denne ret er navnlig relevant, når den

registrerede har givet sit samtykke som barn og ikke er fuldt ud var bekendt med risiciene i forbindelse med behandling, og senere ønsker at fjerne sådanne personoplysninger, særligt på internettet. Den registrerede bør kunne udøve denne rettighed, uanset om vedkommende ikke længere er et barn. Yderligere opbevaring af personoplysningerne bør dog være lovlig, hvis det er nødvendigt for at udøve retten til ytrings- og informationsfrihed, for at overholde en retlig forpligtelse, for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, af hensyn til samfundsinteresser på folkesundhedsområdet, til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller statistiske formål, eller for at retskrav kan fastlægges, gøres gældende eller forsvares.

(66) 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 af 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.

(67) Metoder til at begrænse behandlingen af personoplysninger kan bl.a. 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. 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.

(68) For at give den registrerede øget kontrol over sine personoplysninger bør vedkommende, når behandling af personoplysninger foretages automatisk, også kunne modtage personoplysninger vedrørende vedkommende, som vedkommende har givet til en dataansvarlig, i et struktureret, almindeligt anvendt, maskinlæsbart og indbyrdes kompatibelt format og kunne transmittere dem til en anden dataansvarlig. Dataansvarlige bør opfordres til at udvikle indbyrdes kompatible formater, der muliggør dataportabilitet. Denne ret bør gælde, hvis den registrerede har givet personoplysningerne på grundlag af sit samtykke, eller hvis behandlingen er nødvendig for opfyldelsen af en kontrakt. Den bør ikke gælde, hvis behandlingen er baseret på et andet retsgrundlag end samtykke eller kontrakt. Denne ret bør på grund af selve sin karakter ikke udøves over for dataansvarlige, der behandler personoplysninger under udøvelsen af deres offentlige opgaver. Derfor bør den ikke gælde, hvis behandlingen af personoplysninger er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, eller for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Den registreredes ret til at transmittere eller modtage personoplysninger vedrørende vedkommende bør ikke skabe en forpligtelse for dataansvarlige til at indføre eller opretholde behandlingssystemer, som er teknisk kompatible. Såfremt et sæt personoplysninger vedrører mere end én registreret, bør retten til at modtage personoplysningerne ikke berøre andre registreredes rettigheder og frihedsrettigheder i overensstemmelse med denne forordning. Denne ret bør endvidere ikke berøre den registreredes ret til at få slettet personoplysninger og begrænsningerne i denne ret som fastsat i denne forordning og bør navnlig ikke indebære, at personoplysninger, som den registrerede har givet til opfyldelse af en kontrakt, slettes, i det omfang og så længe personoplysningerne er nødvendige for opfyldelse af kontrakten. Hvis det er teknisk muligt, bør den registrerede have ret til at få personoplysningerne transmitteret direkte fra en dataansvarlig til en anden.

(69) 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.

(70) 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.

(71) 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. 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. Afgørelser baseret på en sådan behandling, herunder profilering, bør dog 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. En sådan behandling bør under alle omstændigheder 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. En sådan foranstaltning bør ikke omfatte et barn.

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. Automatiske afgørelser og profilering baseret på særlige kategorier af personoplysninger bør kun tillades under særlige omstændigheder.

(72) Profilering er omfattet af reglerne i denne forordning vedrørende behandlingen af personoplysninger, såsom retsgrundlaget for behandling og databeskyttelsesprincipper. Det Europæiske Databeskyttelsesråd oprettet ved denne forordning (»Databeskyttelsesrådet«) bør kunne udstede retningslinjer i denne forbindelse.

(73) 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. En sådan begrænsning bør være i overensstemmelse med kravene i chartret og i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder.

(74) Der bør fastsættes bestemmelser om den dataansvarliges ansvar, herunder erstatningsansvar, for enhver behandling af personoplysninger, der foretages af den dataansvarlige eller på den dataansvarliges vegne. Den dataansvarlige bør navnlig have pligt til at gennemføre passende og effektive foranstaltninger og til at påvise, at behandlingsaktiviteter overholder denne forordning, herunder foranstaltningernes effektivitet. Disse foranstaltninger bør tage højde for behandlingens karakter, omfang, sammenhæng og formål og risikoen for fysiske personers rettigheder og frihedsrettigheder.

(75) Risiciene for fysiske personers rettigheder og frihedsrettigheder, af varierende sandsynlighed og alvor, kan opstå som følge af behandling af personoplysninger, der kan føre til fysisk, materiel eller immateriel skade, navnlig hvis behandlingen kan give anledning til forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser; 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.

(76) 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 evalueres på grundlag af en objektiv vurdering, hvorved det fastslås, om databehandlingsaktiviteter indebærer en risiko eller en høj risiko.

(77) Retningslinjer til den dataansvarlige eller databehandleren om implementering af passende foranstaltninger og for påvisning af vedkommendes overholdelse af denne forordning, navnlig for så vidt angår identificering af risikoen i forbindelse med behandlingen, deres vurdering med hensyn til risikoens oprindelse, karakter, sandsynlighed og alvor og om identificering af bedste praksis med henblik på at begrænse denne risiko, kan opstilles, navnlig gennem godkendte adfærdskodekser, godkendte certificeringer, retningslinjer fra Databeskyttelsesrådet eller en databeskyttelsesrådgivers anvisninger. Databeskyttelsesrådet kan også opstille retningslinjer for behandlingsaktiviteter, som anses for sandsynligvis ikke at medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og give anvisninger for, hvilke foranstaltninger der kan være tilstrækkelige i disse tilfælde for at afhjælpe en sådan risiko.

(78) Beskyttelse af fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger kræver, at der træffes passende tekniske og organisatoriske foranstaltninger for at sikre, at denne forordnings krav opfyldes. For at kunne påvise overholdelse af denne forordning bør den dataansvarlige vedtage interne politikker og gennemføre foranstaltninger, som især lever op til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Sådanne foranstaltninger kan bl.a. 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. Når producenter af produkter, tjenester og applikationer udvikler, designer, udvælger og bruger applikationer, tjenester og produkter, der er baseret på behandling af personoplysninger eller behandler personoplysninger, for at udføre deres opgaver, bør de tilskyndes til at tage højde for retten til databeskyttelse i forbindelse med udvikling og design af sådanne produkter, tjenester og applikationer og til under behørig hensyntagen til det aktuelle tekniske niveau at sørge for, at de dataansvarlige og databehandlerne er i stand til at opfylde deres databeskyttelsesforpligtelser. Der bør også tages hensyn til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i forbindelse med offentlige udbud.

(79) 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.

(80) 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. Repræsentanten bør handle på den dataansvarliges eller databehandlerens vegne og kan kontaktes af enhver tilsynsmyndighed. Repræsentanten bør udtrykkelig 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. Udpegelsen af en sådan repræsentant berører ikke den dataansvarliges eller databehandlerens ansvar, herunder erstatningsansvar, i henhold til denne forordning. 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. Den udpegede repræsentant bør være underlagt håndhævelsesforanstaltninger i tilfælde af manglende overholdelse fra den dataansvarliges eller databehandlerens side.

(81) Med henblik på at sikre overholdelse af kravene i denne forordning i forbindelse med behandling, der foretages af en databehandler på vegne af den dataansvarlige, når databehandleren overdrages behandlingsaktiviteter, bør den dataansvarlige udelukkende 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 denne forordning, herunder med hensyn til behandlingssikkerhed. Databehandlerens overholdelse af en godkendt adfærdskodeks eller en godkendt certificeringsmekanisme kan bruges som et element til at påvise, at den dataansvarlige overholder sine forpligtelser. Bestemmelserne om behandling ved en databehandler bør fastsættes i en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der binder databehandleren til den dataansvarlige, og hvori behandlingens genstand og varighed, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede er fastsat, idet der tages hensyn til databehandleres specifikke opgaver og ansvar i forbindelse med den behandling, der skal foretages, og risikoen for den registreredes rettigheder og frihedsrettigheder. Den dataansvarlige og databehandleren kan vælge at anvende en individuel kontrakt eller standardkontraktbestemmelser, der er vedtaget enten direkte af Kommissionen eller af en tilsynsmyndighed i henhold til sammenhængsmekanismen og derefter vedtaget af Kommissionen. Databehandleren bør efter den dataansvarliges valg tilbagelevere eller slette de pågældende personoplysninger efter afslutning af den behandling, der er foretaget på vegne af den dataansvarlige, medmindre der er et krav om at opbevare personoplysningerne i EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt.

(82) For at påvise overholdelse af denne forordning bør den dataansvarlige eller databehandleren 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.

(83) 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 personoplysninger, 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.

(84) 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.

(85) 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. Så

snart den dataansvarlige bliver bekendt med, at der er sket et brud på persondatasikkerheden, bør vedkommende derfor anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed uden unødig forsinkelse og om muligt senest 72 timer efter, at denne er blevet bekendt med det, medmindre den dataansvarlige i overensstemmelse med ansvarlighedsprincippet kan påvise, at bruddet på persondatasikkerheden sandsynligvis ikke indebærer risiko for fysiske personers rettigheder eller frihedsrettigheder. Hvis en sådan anmeldelse ikke kan ske inden for 72 timer, bør den ledsages af en begrundelse for forsinkelsen, og oplysningerne kan indgives trinvis uden unødig yderligere forsinkelse.

(86) Den dataansvarlige bør underrette den registrerede om et brud på persondatasikkerheden uden unødig forsinkelse, når dette brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for den fysiske persons rettigheder og frihedsrettigheder, med henblik på at give vedkommende mulighed for at træffe de fornødne forholdsregler. Underretningen bør beskrive karakteren af bruddet på persondatasikkerheden og indeholde anbefalinger til den berørte fysiske person med henblik på at begrænse de mulige skadevirkninger. Sådanne 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.

(87) Det bør undersøges, om alle passende teknologiske beskyttelsesforanstaltninger og organisatoriske foranstaltninger er blevet gennemført, for omgående at kunne fastslå, om et brud på persondatasikkerheden har fundet sted, og for straks at kunne informere tilsynsmyndigheden og den registrerede. 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. En sådan anmeldelse kan føre til indgriben fra tilsynsmyndigheden i overensstemmelse med dens opgaver og beføjelser i henhold til denne forordning.

(88) Når der fastsættes nærmere regler for, hvilket format og hvilke procedurer der skal anvendes ved anmeldelse af brud på persondatasikkerheden, bør der 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.

(89) Ved direktiv 95/46/EF blev der 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.

(90) I sådanne tilfælde bør den dataansvarlige inden behandlingen 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.

(91) Dette er især relevant i forbindelse med omfattende behandlingsaktiviteter 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 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.

Der bør også 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. En konsekvensanalyse vedrørende databeskyttelse er ligeledes 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. Behandling af personoplysninger bør ikke 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.

(92) 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.

(93) 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 medlemsstaterne vurdere, at en sådan analyse skal foretages inden behandlingsaktiviteterne.

(94) 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 og 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.

(95) Databehandleren bør bistå den dataansvarlige, når det er nødvendigt og efter anmodning, med at sikre overholdelse af de forpligtelser, der udspringer af foretagelse af konsekvensanalyser vedrørende databeskyttelse og forudgående høring af tilsynsmyndigheden.

(96) Tilsynsmyndigheden bør ligeledes 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 denne forordning, og navnlig for at begrænse risiciene for den registrerede.

(97) Hvis behandling foretages af en offentlig myndighed, bortset fra domstole eller andre uafhængige judicielle myndigheder, når de handler i deres egenskab af domstol, hvis behandling i den private sektor foretages af en dataansvarlig, hvis kerneaktiviteter består i behandlingsaktiviteter, som kræver regelmæssig og systematisk overvågning af de registrerede i stort omfang, eller hvis den dataansvarliges eller databehandlerens kerneaktiviteter består af behandling i stort omfang af særlige kategorier af oplysninger og oplysninger vedrørende straffedomme og lovovertrædelser, bør en person med ekspertise i databeskyttelsesret og -praksis bistå den dataansvarlige eller databehandleren med at overvåge den interne overholdelse af denne forordning. I den private sektor vedrører en dataansvarligs kerneaktiviteter vedkommendes hovedaktiviteter og ikke behandling af personoplysninger som biaktivitet. Den nødvendige ekspertise bør navnlig fastlægges i henhold til de databehandlingsaktiviteter, der

foretages, og den beskyttelse de personoplysninger, som den dataansvarlige eller databehandleren behandler, kræver. Sådanne databeskyttelsesrådgivere bør, uanset om de er ansat hos den dataansvarlige eller ej, være i stand til at udøve deres hverv på uafhængig vis.

(98) 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. Sådanne adfærdskodekser bør navnlig 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.

(99) 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.

(100) For at forbedre gennemsigtigheden og overholdelsen af denne forordning bør fastlæggelsen af certificeringsmekanismer og databeskyttelsesmærkninger og -mærker fremmes, så registrerede hurtigt kan vurdere databeskyttelsesniveauet i forbindelse med relevante produkter og tjenester.

(101) Strømmen af personoplysninger til og fra lande uden for Unionen og til og fra internationale organisationer er nødvendig af hensyn til udbygningen af den internationale samhandel og det internationale samarbejde. Udvidelsen af denne strøm har skabt nye udfordringer og betænkeligheder med hensyn til beskyttelsen af personoplysninger. Når personoplysninger overføres fra Unionen til dataansvarlige, databehandlere eller andre modtagere i tredjelande eller til internationale organisationer, må det beskyttelsesniveau, som fysiske personer sikres i Unionen i medfør af denne forordning, dog ikke undermineres, herunder i tilfælde af videreoverførsel af personoplysninger fra et tredjeland eller en international organisation til dataansvarlige, databehandlere i det samme eller et andet tredjeland eller en anden international organisation. Overførsel til tredjelande og internationale organisationer må under alle omstændigheder kun finde sted under fuld overholdelse af denne forordning. En overførsel vil kun kunne finde sted, hvis den dataansvarlige eller databehandleren opfylder betingelserne i denne forordning vedrørende overførsel af personoplysninger til tredjelande eller internationale organisationer, jf. dog de øvrige bestemmelser i denne forordning.

(102) Denne forordning berører ikke internationale aftaler indgået mellem Unionen og tredjelande om overførsel af personoplysninger, herunder de fornødne garantier for registrerede. Medlemsstaterne kan indgå internationale aftaler, som omfatter overførsel af personoplysninger til tredjelande eller internationale organisationer, for så vidt sådanne aftaler ikke berører denne forordning eller andre bestemmelser i EU-retten og omfatter et passende beskyttelsesniveau for registreredes grundlæggende rettigheder.

(103) Kommissionen kan med virkning for hele Unionen træffe afgørelse om, at et tredjeland, et område eller en specifik sektor i et tredjeland, eller en international organisation har et tilstrækkeligt databeskyttelsesniveau, og dermed skabe retssikkerhed og ensartethed i hele Unionen hvad angår det tredjeland eller den internationale organisation, der vurderes at have et sådant beskyttelsesniveau. I sådanne tilfælde kan personoplysninger overføres til det pågældende tredjeland uden yderligere godkendelse. Kommissionen kan også træffe afgørelse om at tilbagekalde en sådan afgørelse efter at have underrettet og fyldestgørende begrundet det over for det pågældende tredjeland eller den pågældende internationale organisation.

(104) I overensstemmelse med de grundlæggende værdier, som Unionen bygger på, navnlig beskyttelse af menneskerettighederne, bør Kommissionen i sin vurdering af et tredjeland eller et område eller en specifik sektor i et tredjeland tage hensyn til, hvordan et bestemt tredjeland efterlever retsstatsprincippet, klageadgang og domstolsprøvelse, internationale menneskerettighedsnormer og -standarder samt sin generelle og sektorbestemte ret, herunder lovgivning vedrørende offentlig sikkerhed, forsvar, statens sikkerhed samt offentlig orden og strafferet. Når der vedtages en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i et område eller en specifik sektor i et tredjeland, bør der tages hensyn til klare og objektive kriterier, som f.eks. specifikke behandlingsaktiviteter og anvendelsesområdet for gældende retsstandarder og lovgivning i tredjelandet. Tredjelandet bør give

garantier, der sikrer et passende beskyttelsesniveau, som i det væsentlige svarer til det, der sikres i Unionen, især når personoplysninger behandles i en eller flere specifikke sektorer. Tredjelandet bør navnlig sikre et effektivt uafhængigt databeskyttelsestilsyn og bør fastlægge samarbejdsmekanismer med medlemsstaternes databeskyttelsesmyndigheder, og de registrerede bør have effektive rettigheder, som kan håndhæves, og adgang til effektiv administrativ og retslig prøvelse.

(105) Ud over de internationale forpligtelser, som tredjelandet eller den internationale organisation har indgået, bør Kommissionen tage hensyn til forpligtelser, der følger af tredjelandets eller den internationale organisations deltagelse i multilaterale eller regionale systemer, navnlig i forbindelse med beskyttelse af personoplysninger, samt gennemførelsen af sådanne forpligtelser. Der bør navnlig tages hensyn til tredjelandets tiltrædelse af Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger og tillægsprotokollen hertil. Kommissionen bør høre Databeskyttelsesrådet, når den vurderer beskyttelsesniveauet i tredjelande eller internationale organisationer.

(106) Kommissionen bør overvåge virkningen af afgørelser om beskyttelsesniveauet i et tredjeland, et område eller en specifik sektor i et tredjeland, eller en international organisation, og overvåge virkningen af afgørelser vedtaget på grundlag af artikel 25, stk. 6, eller artikel 26, stk. 4, i direktiv 95/46/EF. I sine afgørelser om tilstrækkeligheden af beskyttelsesniveauet bør Kommissionen fastsætte en mekanisme for regelmæssig revision af afgørelsernes virkning. Denne regelmæssige revision bør foretages i samråd med det pågældende tredjeland eller den pågældende internationale organisation og tage hensyn til enhver relevant udvikling i tredjelandet eller den internationale organisation. I forbindelse med overvågning og den regelmæssige revision bør Kommissionen tage hensyn til synspunkter og resultater fra Europa-Parlamentet og fra Rådet såvel som fra andre relevante organer og kilder. Kommissionen bør inden for en rimelig frist evaluere virkningen af sidstnævnte afgørelser og rapportere alle relevante resultater til det udvalg som er omhandlet i Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 ([1]), der nedsættes ved nærværende forordning, og til Europa-Parlamentet og Rådet.

(107) Kommissionen kan fastslå, at et tredjeland, et område eller en specifik sektor i et tredjeland, eller en international organisation ikke længere sikrer et tilstrækkeligt databeskyttelsesniveau. Overførsel af personoplysninger til et sådant tredjeland eller en sådan international organisation bør derfor forbydes, medmindre kravene i denne forordning vedrørende overførsel omfattet af fornødne garantier, herunder bindende virksomhedsregler og undtagelser i særlige situationer, er opfyldt. Der bør i sådanne tilfælde fastlægges bestemmelser om en procedure for konsultationer mellem Kommissionen og sådanne tredjelande eller internationale organisationer. Kommissionen bør rettidigt underrette tredjelandet eller den internationale organisation om årsagerne og indlede konsultationer med tredjelandet eller den internationale organisation for at afhjælpe situationen.

(108) I mangel af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet bør den dataansvarlige eller databehandleren træffe foranstaltninger for at kompensere for den manglende databeskyttelse i et tredjeland i form af fornødne garantier for den registrerede. Sådanne fornødne garantier kan bestå i anvendelse af bindende virksomhedsregler, standardbestemmelser om databeskyttelse vedtaget af Kommissionen, standardbestemmelser om databeskyttelse vedtaget af en tilsynsmyndighed eller kontraktbestemmelser godkendt af en tilsynsmyndighed. Disse garantier bør sikre overholdelse af databeskyttelseskravene og de registreredes rettigheder i forbindelse med intern behandling i Unionen, herunder tilgængelighed af rettigheder, som kan håndhæves, for registrerede og effektive retsmidler, herunder til at opnå effektiv administrativ eller retslig prøvelse og til at kræve erstatning, i Unionen eller et tredjeland. Garantierne bør navnlig vedrøre overholdelse af de generelle principper for behandling af personoplysninger og principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Overførsel kan også foretages af offentlige myndigheder eller organer til offentlige myndigheder eller organer i tredjelande eller til internationale organisationer med tilsvarende opgaver eller funktioner, herunder på grundlag af bestemmelser, der medtages i administrative ordninger, f.eks. et aftalememorandum, hvorved de registrerede sikres effektive rettigheder, som kan håndhæves. Godkendelse fra den kompetente tilsynsmyndighed bør indhentes, når garantierne indgår i administrative ordninger, der ikke er juridisk bindende.

(109) Den dataansvarliges eller databehandlerens mulighed for at bruge standardbestemmelser om databeskyttelse vedtaget af Kommissionen eller en tilsynsmyndighed bør hverken udelukke muligheden for, at den dataansvarlige

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

eller databehandleren medtager standardbestemmelser om databeskyttelse i en bredere kontrakt, såsom en kontrakt mellem databehandleren og en anden databehandler, eller medtager andre bestemmelser eller yderligere garantier, såfremt de hverken direkte eller indirekte er i strid med de standardkontraktbestemmelser, der er vedtaget af Kommissionen eller en tilsynsmyndighed, eller berører de registreredes grundlæggende rettigheder eller frihedsrettigheder. Dataansvarlige og databehandlere bør tilskyndes til at give yderligere garantier gennem kontraktmæssige forpligtelser, der supplerer standardbestemmelserne om beskyttelse.

(110) 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.

(111) Overførsel bør tillades under visse omstændigheder, når den registrerede har givet sit udtrykkelige samtykke, og hvor overførsel er lejlighedsvis og nødvendig i forbindelse med en kontrakt eller et retskrav, uanset om det sker i forbindelse med en retssag eller en administrativ eller udenretslig procedure, herunder procedurer ved reguleringsorganer. Overførsel bør også tillades, når vigtige samfundsinteresser i henhold til EU-retten eller medlemsstaternes nationale ret kræver det, eller når overførsel sker fra et register, der er oprettet ved lov, og som er tilgængeligt for offentligheden eller personer med en legitim interesse. I sidstnævnte tilfælde bør sådan overførsel ikke omfatte alle personoplysningerne eller alle kategorier af oplysninger i registeret, og når registeret er beregnet til at blive konsulteret af personer, der har en legitim interesse, bør overførsel under fuld hensyntagen til den registreredes interesser og grundlæggende rettigheder kun ske på anmodning af disse personer, eller hvis de skal være modtagere.

(112) Disse fravigelser bør navnlig gælde for overførsel af oplysninger, der foretages af hensyn til vigtige samfundsinteresser, f.eks. international udveksling af oplysninger mellem konkurrencemyndigheder, skatte- eller toldforvaltninger, finansielle tilsynsmyndigheder eller socialsikringsmyndigheder eller med henblik på folkesundhed, f.eks. i tilfælde af kontaktopsporing i forbindelse med smitsomme sygdomme eller for at nedbringe og/eller afskaffe doping inden for sport. Overførsel af personoplysninger, der er nødvendig for at beskytte et hensyn af fundamental betydning for den registreredes eller en anden persons vitale interesser, herunder fysisk integritet eller liv, bør ligeledes anses for lovlig, hvis den registrerede er ude af stand til at give sit samtykke. I mangel af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet kan EU-retten eller medlemsstaternes nationale ret af hensyn til vigtige samfundsinteresser udtrykkelig fastsætte grænser for overførsel af særlige kategorier af oplysninger til et tredjeland eller en international organisation. Medlemsstaterne bør give Kommissionen meddelelse om sådanne bestemmelser. Enhver overførsel til en international humanitær organisation af personoplysninger om en registreret, der ikke fysisk eller juridisk er i stand til at give sit samtykke, med henblik på udførelse af en opgave i henhold til Genèvekonventionerne eller for at overholde international humanitær ret, som finder anvendelse i væbnede konflikter, kan anses for at være nødvendig af hensyn til vigtige samfundsinteresser, eller fordi det er af vital interesse for den registrerede.

(113) Overførsler, der ikke kan betegnes som værende præget af gentagelser, og som kun vedrører et begrænset antal registrerede, kan også være mulig af hensyn til vægtige legitime interesser, som forfølges af den dataansvarlige, hvis den registreredes interesser eller rettigheder og frihedsrettigheder ikke går forud for disse interesser, og hvis den dataansvarlige har vurderet alle omstændigheder i forbindelse med overførslen. Den dataansvarlige bør lægge særlig vægt på de pågældende personoplysningers karakter, formålet med og varigheden af den eller de foreslåede behandlinger samt situationen i oprindelseslandet, tredjelandet og det endelige bestemmelsesland og bør give fornødne garantier for beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder med hensyn til behandling af deres personoplysninger. Sådan overførsel bør kun være mulig i enkelttilfælde, hvor ingen af de andre grunde til overførsel kan finde anvendelse. Med henblik på videnskabelige eller historiske forskningsformål eller statistiske formål bør samfundets legitime forventninger om øget viden tages med i overvejelserne. Den dataansvarlige bør underrette tilsynsmyndigheden og den registrerede om overførslen.

(114) Hvis Kommissionen ikke har truffet afgørelse om tilstrækkeligheden af databeskyttelsesniveauet i et tredjeland, bør den dataansvarlige eller databehandleren under alle omstændigheder benytte løsninger, der giver de registrerede effektive rettigheder, som kan håndhæves, hvad angår behandlingen af deres personoplysninger i Unionen, når disse oplysninger er blevet overført, så de fortsat vil nyde godt af grundlæggende rettigheder og garantier.

(115) Visse tredjelande vedtager love, forskrifter og andre retsakter med det formål direkte at regulere behandlingsaktiviteter udøvet af fysiske og juridiske personer under medlemsstaternes jurisdiktion. Dette kan omfatte retsafgørelser eller administrative myndigheders afgørelser i tredjelande, der kræver, at en dataansvarlig eller en databehandler overfører personoplysninger, og som ikke er baseret på en gældende international aftale som en traktat om gensidig retshjælp mellem det anmodende tredjeland og Unionen eller en medlemsstat. Ekstraterritorial anvendelse af sådanne love, forskrifter og andre retsakter kan være i strid med folkeretten og hindre opnåelse af den beskyttelse af fysiske personer, der sikres i Unionen ved denne forordning. Overførsel af oplysninger bør kun tillades, hvis denne forordnings betingelser for overførsel til tredjelande er opfyldt. Det kan være tilfældet, bl.a. hvis videregivelse er nødvendig af hensyn til vigtige samfundsinteresser, der anerkendes i EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er omfattet af.

(116) Når personoplysninger overføres på tværs af grænser uden for Unionen, kan det medføre yderligere risici for fysiske personers mulighed for at udøve deres databeskyttelsesrettigheder og beskytte sig mod ulovlig brug eller videregivelse af disse oplysninger. Samtidig må tilsynsmyndighederne i nogle tilfælde konstatere, at de er ude af stand til at følge op på klager eller foretage undersøgelser vedrørende aktiviteter uden for deres grænser. Samarbejdet på tværs af grænserne kan også hæmmes af utilstrækkelige forebyggende eller afhjælpende beføjelser, uensartede retlige ordninger og praktiske hindringer som f.eks. ressourcebegrænsninger. Der er derfor behov for at fremme tættere samarbejde mellem datatilsynsmyndigheder, så de bedre kan udveksle oplysninger og gennemføre undersøgelser sammen med de tilsvarende internationale organer. Med henblik på at udvikle mekanismer for internationalt samarbejde for at lette og yde international gensidig bistand til håndhævelsen af lovgivning om beskyttelse af personoplysninger bør Kommissionen og tilsynsmyndighederne udveksle oplysninger og samarbejde om aktiviteter i forbindelse med udøvelsen af deres beføjelser med de kompetente myndigheder i tredjelande på grundlag af gensidighed og i overensstemmelse med denne forordning.

(117) 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. Medlemsstaterne bør kunne oprette mere end én tilsynsmyndighed for at afspejle deres forfatningsmæssige, organisatoriske og administrative struktur.

(118) Tilsynsmyndighedernes uafhængighed bør ikke betyde, at tilsynsmyndighederne ikke kan underkastes kontrol eller tilsynsmekanismer hvad angår deres finansielle udgifter eller underkastes domstolskontrol.

(119) Hvis en medlemsstat opretter flere tilsynsmyndigheder, bør den ved lov fastlægge mekanismer, der sikrer disse tilsynsmyndigheders effektive deltagelse i sammenhængsmekanismen. Den pågældende medlemsstat bør navnlig udpege den tilsynsmyndighed, der fungerer som fælles kontaktpunkt for disse myndigheders effektive deltagelse i mekanismen, med henblik på at sikre et hurtigt og smidigt samarbejde med andre tilsynsmyndigheder, Databeskyttelsesrådet og Kommissionen.

(120) Hver tilsynsmyndighed bør have de nødvendige finansielle og menneskelige ressourcer samt lokaler og infrastruktur til effektivt at kunne udføre sine opgaver, herunder opgaver vedrørende gensidig bistand og samarbejde med andre tilsynsmyndigheder i hele Unionen. Hver tilsynsmyndighed bør have et separat offentligt årligt budget, der kan indgå i det samlede statsbudget eller nationale budget.

(121) De generelle betingelser for en tilsynsmyndigheds medlem eller medlemmer bør fastsættes ved lov i hver medlemsstat og bør navnlig fastsætte, at disse medlemmer skal udnævnes ved en gennemsigtig procedure enten af parlamentet, regeringen eller statschefen i den pågældende medlemsstat på grundlag af et forslag fra regeringen, et medlem af regeringen, parlamentet eller et kammer i parlamentet eller af et uafhængigt organ, der har bemyndigelse hertil i henhold til medlemsstaternes nationale ret. For at sikre tilsynsmyndighedens uafhængighed bør medlemmet eller medlemmerne handle med integritet, afholde sig fra enhver handling, der er uforenelig med deres hverv, og ikke, så længe deres embedsperiode varer, udøve uforenelig lønnet eller ulønnet virksomhed. Tilsynsmyndigheden bør have sit eget personale, der er udvalgt af tilsynsmyndigheden eller et uafhængigt organ, der er oprettet ved medlemsstaternes nationale ret, og som udelukkende bør være underlagt tilsynsmyndighedens medlems eller medlemmers ledelse.

(122) Hver tilsynsmyndighed bør på sin egen medlemsstats område have kompetence til at udøve sine beføjelser og varetage de opgaver, der er tildelt den i henhold til denne forordning. Dette bør navnlig omfatte behandling, som

foretages som led i aktiviteter, der udføres for den dataansvarliges eller databehandlerens etablering på dens egen medlemsstats område, behandling af personoplysninger, der udføres af offentlige myndigheder eller af private organer i offentlighedens interesse, behandling, der påvirker registrerede på dens område, eller behandling, der udføres af en dataansvarlig eller en databehandler, som ikke er etableret i Unionen, når den er rettet mod registrerede, som har bopæl på dens område. Dette bør omfatte behandling af klager, der er indgivet af en registreret, udførelse af undersøgelser vedrørende denne forordnings anvendelse og en indsats for at fremme offentlighedens bevidstgørelse om risici, regler, garantier og rettigheder i forbindelse med behandling af personoplysninger.

(123) Tilsynsmyndighederne bør føre tilsyn med anvendelsen af bestemmelserne i henhold til denne forordning og bidrage til ensartet anvendelse heraf i hele Unionen for at beskytte fysiske personer i forbindelse med behandling af deres personoplysninger og lette fri udveksling af personoplysninger på det indre marked. Til det formål bør tilsynsmyndighederne samarbejde med hinanden og Kommissionen, uden at der er behov for en aftale mellem medlemsstater om gensidig bistand eller om et sådant samarbejde.

(124) Hvis behandling af personoplysninger foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, der er etableret i Unionen, og den dataansvarlige eller databehandleren er etableret i mere end én medlemsstat, eller hvis den behandling, der finder sted som led i aktiviteter, som udføres for en dataansvarlig eller en databehandler, som kun er etableret i én medlemsstat i Unionen, og behandlingen i væsentlig grad påvirker eller sandsynligvis i væsentlig grad vil påvirke registrerede i mere end én medlemsstat, bør tilsynsmyndigheden for den dataansvarliges eller databehandlerens hovedvirksomhed eller for den dataansvarliges eller databehandlerens eneste etablering i Unionen fungere som ledende tilsynsmyndighed. Den ledende tilsynsmyndighed bør samarbejde med de andre berørte myndigheder, fordi den dataansvarlige eller databehandleren har en etablering på deres medlemsstats område, fordi de registrerede, der har bopæl på deres område, er påvirket i væsentlig grad, eller fordi der er blevet indgivet en klage til dem. Også hvis en registreret, der ikke har bopæl i den medlemsstat, har indgivet en klage, bør den tilsynsmyndighed, til hvem klagen er indgivet, være en berørt tilsynsmyndighed. Databeskyttelsesrådet bør inden for rammerne af sine opgaver med at udstede retningslinjer om ethvert spørgsmål vedrørende anvendelsen af denne forordning navnlig 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.

(125) Den ledende tilsynsmyndighed bør have kompetence til at vedtage bindende afgørelser vedrørende foranstaltninger, der anvender de beføjelser, den er tillagt i overensstemmelse med denne forordning. Tilsynsmyndigheden bør i sin egenskab af ledende tilsynsmyndighed nøje inddrage og koordinere de berørte tilsynsmyndigheder i beslutningsprocessen. Hvis der træffes afgørelse om helt eller delvist at afvise den registreredes klage, bør denne afgørelse vedtages af den tilsynsmyndighed, til hvem klagen er indgivet.

(126) Afgørelsen bør træffes i fællesskab af den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder og bør være rettet mod den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering samt være bindende for den dataansvarlige og databehandleren. Den dataansvarlige eller databehandleren bør træffe de nødvendige foranstaltninger til at sikre overholdelse af denne forordning samt gennemførelse af den afgørelse, som af den ledende tilsynsmyndighed meddeles den dataansvarlige eller databehandlerens hovedvirksomhed for så vidt angår behandlingsaktiviteter i Unionen.

(127) Hver tilsynsmyndighed, der ikke fungerer som den ledende tilsynsmyndighed, bør være kompetent til at behandle lokale sager, hvis den dataansvarlige eller databehandleren er etableret i mere end én medlemsstat, men genstanden for den specifikke behandling kun vedrører behandling i én medlemsstat og kun vedrører registrerede i denne ene medlemsstat, f.eks. hvis genstanden er behandling af arbejdstageres personoplysninger i en bestemt beskæftigelsessammenhæng i en medlemsstat. I sådanne tilfælde bør tilsynsmyndigheden straks underrette den ledende tilsynsmyndighed om forholdet. Efter at være blevet underrettet bør den ledende tilsynsmyndighed afgøre, om den vil behandle sagen i medfør af bestemmelsen om samarbejde mellem den ledende tilsynsmyndighed og andre berørte tilsynsmyndigheder (»one-stop-shop mekanismen«), eller om den tilsynsmyndighed, der underrettede den, bør behandle sagen på lokalt plan. Når den ledende tilsynsmyndighed afgør, om den vil behandle sagen, bør den tage hensyn til, om den dataansvarlige eller databehandleren er etableret i medlemsstaten for den tilsynsmyndighed, der underrettede den, med henblik på at sikre effektiv håndhævelse af en afgørelse over for den dataansvarlige eller databehandleren. Hvis den ledende tilsynsmyndighed

beslutter at behandle sagen, bør den tilsynsmyndighed, der underrettede den, have mulighed for at forelægge et udkast til afgørelse, som den ledende tilsynsmyndighed bør tage størst muligt hensyn til ved udarbejdelsen af sit udkast til afgørelse inden for denne one-stop-shop mekanisme.

(128) Reglerne om den ledende tilsynsmyndighed og one-stop-shop mekanismen bør ikke gælde, når behandling foretages af offentlige myndigheder eller af private organer i offentlighedens interesse. I sådanne tilfælde bør kun tilsynsmyndigheden i den medlemsstat, hvor den offentlige myndighed eller det private organ er etableret, have kompetence til at udøve de beføjelser, som den er tillagt i henhold til denne forordning.

(129) For at sikre ensartet tilsyn med og håndhævelse af denne forordning i hele Unionen bør tilsynsmyndighederne i hver medlemsstat have samme opgaver og effektive beføjelser, herunder undersøgelsesbeføjelser og beføjelser til at fastsætte korrigerende foranstaltninger og sanktioner samt godkendelses- og rådgivningsbeføjelser, navnlig i tilfælde af klager fra fysiske personer, og med forbehold for de retsforfølgende myndigheders beføjelser i henhold til medlemsstaternes nationale ret, til at indbringe overtrædelser af denne forordning for de judicielle myndigheder og deltage i retssager. Disse beføjelser bør også omfatte beføjelse til midlertidig eller definitivt at begrænse, herunder forbyde, behandling. Medlemsstaterne kan fastsætte andre opgaver, som vedrører beskyttelse af personoplysninger i henhold til denne forordning. Tilsynsmyndighedernes beføjelser bør udøves i overensstemmelse med de fornødne proceduremæssige garantier, der er fastsat i EU-retten og medlemsstaternes nationale ret, uvildigt, retfærdigt og inden for en rimelig frist. Hver foranstaltning bør især være passende, nødvendig og forholdsmæssig for at sikre overholdelse af denne forordning, idet der tages hensyn til omstændighederne i hver enkelt sag, bør overholde enhver persons ret til at blive hørt, inden der træffes en individuel foranstaltning, som vil berøre den pågældende negativt, og bør undgå overflødige udgifter og urimelige ulemper for de berørte personer. Hvad angår adgang til lokaler bør undersøgelsesbeføjelserne udøves i overensstemmelse med specifikke krav i medlemsstaternes retspleje, f.eks. krav om en forudgående retskendelse. Hver juridisk bindende foranstaltning, der træffes af en tilsynsmyndighed, bør være skriftlig, klar og utvetydig, angive navnet på den tilsynsmyndighed, der har truffet foranstaltningen, og datoen for iværksættelse af foranstaltningen, være underskrevet af chefen for eller et medlem af tilsynsmyndigheden, som vedkommende har givet bemyndigelse hertil, angive begrundelsen for foranstaltningen og indeholde en henvisning til adgang til effektive retsmidler. Dette bør ikke udelukke yderligere krav i medfør af medlemsstaternes retspleje. Vedtagelse af en juridisk bindende afgørelse indebærer, at den kan undergives domstolskontrol i medlemsstaten for den tilsynsmyndighed, der har vedtaget afgørelsen.

(130) Hvis den tilsynsmyndighed, til hvem en klage er indgivet, ikke er den ledende tilsynsmyndighed, bør den ledende tilsynsmyndighed samarbejde tæt med den tilsynsmyndighed, til hvem klagen er indgivet, i overensstemmelse med bestemmelserne om samarbejde og sammenhæng i denne forordning. I sådanne tilfælde bør den ledende tilsynsmyndighed, når den træffer foranstaltninger, der skal have retsvirkning, herunder pålæggelse af administrative bøder, tage størst muligt hensyn til synspunkterne hos den tilsynsmyndighed, til hvem klagen er indgivet, og som fortsat bør være kompetent til at foretage undersøgelser på sin egen medlemsstats område i samråd med den ledende tilsynsmyndighed.

(131) Hvis en anden tilsynsmyndighed burde fungere som ledende tilsynsmyndighed i forbindelse med den dataansvarliges eller databehandlerens behandlingsaktiviteter, men en klages konkrete indhold eller en mulig overtrædelse kun vedrører den dataansvarliges eller databehandlerens behandlingsaktiviteter i den medlemsstat, hvor klagen er indgivet, eller den konstaterede mulige overtrædelse og forholdet ikke i væsentlig grad påvirker eller sandsynligvis ikke i væsentlig grad vil påvirke registrerede i andre medlemsstater, bør den tilsynsmyndighed, der modtager en klage eller konstaterer eller på anden måde underrettes om situationer, som indebærer mulige overtrædelser af denne forordning, søge at nå frem til en mindelig løsning med den dataansvarlige, og hvis dette ikke lykkes, udøve alle sine beføjelser. Dette bør omfatte specifik behandling, der foretages på tilsynsmyndighedens medlemsstats område eller for så vidt angår registrerede på den pågældende medlemsstats område, behandling, der foretages som led i udbud af varer eller tjenesteydelser specifikt rettet mod registrerede på tilsynsmyndighedens medlemsstats område, eller behandling som skal vurderes under hensyntagen til relevante retlige forpligtelser i henhold til medlemsstaternes nationale ret.

(132) Tilsynsmyndigheders oplysningskampagner over for offentligheden bør omfatte specifikke foranstaltninger rettet mod dataansvarlige og databehandlere, herunder mikrovirksomheder og små og mellemstore virksomheder, samt fysiske personer, navnlig i uddannelsessammenhæng.

(133) Tilsynsmyndighederne bør bistå hinanden i forbindelse med udførelsen af deres opgaver og yde gensidig bistand for at sikre ensartet anvendelse og håndhævelse af denne forordning på det indre marked. En tilsynsmyndighed, der har anmodet om gensidig bistand, kan vedtage en foreløbig foranstaltning, hvis den ikke har modtaget svar på en anmodning om gensidig bistand inden for en måned fra den anden tilsynsmyndigheds modtagelse af anmodningen.

(134) Hver tilsynsmyndighed bør, hvis det er relevant, deltage i fælles aktiviteter sammen med andre tilsynsmyndigheder. En tilsynsmyndighed, der modtager en anmodning, bør være forpligtet til at besvare anmodningen inden for en angiven frist.

(135) For at sikre ensartet anvendelse af denne forordning i hele Unionen bør der etableres en sammenhængsmekanisme for samarbejde mellem tilsynsmyndighederne. Denne mekanisme bør navnlig anvendes, når en tilsynsmyndighed agter at vedtage en foranstaltning, der skal have retsvirkning, i forhold til behandlingsaktiviteter, der i væsentlig grad påvirker et betydeligt antal registrerede i flere medlemsstater. Den bør også anvendes, hvis en berørt tilsynsmyndighed eller Kommissionen ønsker, at en sådan sag behandles inden for sammenhængsmekanismen. Denne mekanisme berører ikke foranstaltninger, som Kommissionen måtte træffe som led i udøvelsen af sine beføjelser i henhold til traktaterne.

(136) I forbindelse med anvendelsen af sammenhængsmekanismen bør Databeskyttelsesrådet inden for en bestemt frist afgive en udtalelse, hvis det besluttes af et flertal af dets medlemmer, eller hvis en berørt tilsynsmyndighed eller Kommissionen anmoder herom. Databeskyttelsesrådet bør også tillægges beføjelse til at vedtage juridisk bindende afgørelser i tilfælde af tvister mellem tilsynsmyndigheder. Til dette formål bør Databeskyttelsesrådet i princippet med et flertal på to tredjedele af sine medlemmer vedtage juridisk bindende afgørelser i klart angivne tilfælde, hvor der er modstridende synspunkter blandt tilsynsmyndighederne, særlig i samarbejdsmekanismen mellem den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder om en sags realitet, navnlig hvorvidt der foreligger en overtrædelse af denne forordning.

(137) Det kan være nødvendigt at handle omgående for at beskytte registreredes rettigheder og frihedsrettigheder, navnlig hvis der er fare for væsentlig vanskeliggørelse af håndhævelsen af en registerets rettigheder. En tilsynsmyndighed bør derfor kunne vedtage behørigt begrundede foreløbige foranstaltninger på sit område med en angivet gyldighedsperiode, der ikke bør overstige tre måneder.

(138) Anvendelse af sammenhængsmekanismen bør være en betingelse for lovligheden af en af en tilsynsmyndighed truffet foranstaltning, der skal have retsvirkning, i tilfælde, hvor anvendelse heraf er obligatorisk. I andre tilfælde af grænseoverskridende relevans bør mekanismen for samarbejde mellem den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder finde anvendelse, og gensidig bistand og fælles aktiviteter kan gennemføres mellem de berørte tilsynsmyndigheder på bilateralt eller multilateralt grundlag, uden at det udløser sammenhængsmekanismen.

(139) Med henblik på at fremme, at denne forordning anvendes på en ensartet måde, bør Databeskyttelsesrådet oprettes som et uafhængigt EU-organ. Databeskyttelsesrådet bør for at kunne opfylde sine målsætninger have status som juridisk person. Det bør repræsenteres af sin formand. Databeskyttelsesrådet bør erstatte Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved direktiv 95/46/EF. Det bør sammensættes af chefen for en tilsynsmyndighed i hver medlemsstat og Den Europæiske Tilsynsførende for Databeskyttelse eller deres respektive repræsentanter. Kommissionen bør deltage i Databeskyttelsesrådets aktiviteter uden stemmeret, og Den Europæiske Tilsynsførende for Databeskyttelse bør have særlige stemmerettigheder. Databeskyttelsesrådet bør bidrage til ensartet anvendelse af denne forordning i hele Unionen, herunder ved at rådgive Kommissionen, navnlig om beskyttelsesniveauet i tredjelande eller internationale organisationer, og fremme samarbejdet mellem tilsynsmyndighederne i hele Unionen. Databeskyttelsesrådet bør handle uafhængigt, når det udfører sine opgaver.

(140) Databeskyttelsesrådet bør bistås af et sekretariat, som stilles til rådighed af Den Europæiske Tilsynsførende for Databeskyttelse. Det personale hos Den Europæiske Tilsynsførende for Databeskyttelse, der deltager i udførelsen af de opgaver, som Databeskyttelsesrådet tildeles ved denne forordning, bør udelukkende udføre sine opgaver efter instruks fra formanden for Databeskyttelsesrådet og rapportere til denne.

(141) Enhver registreret bør have ret til at indgive klage til en enkelt tilsynsmyndighed, navnlig i den medlemsstat, hvor vedkommende har sit sædvanlige opholdssted, og have adgang til effektive retsmidler i overensstemmelse med

artikel 47 i chartret, hvis den registrerede finder, at vedkommendes rettigheder i henhold til denne forordning er blevet krænket, eller hvis tilsynsmyndigheden ikke reagerer på en klage, delvist eller helt afslår eller afviser en klage eller ikke handler, hvis handling er nødvendig for at beskytte den registreredes rettigheder. Undersøgelse af en klage bør foretages i det omfang, det er passende i det specifikke tilfælde, med forbehold af domstolskontrol. Tilsynsmyndigheden bør underrette den registrerede om forløbet og resultatet af klagen inden for en rimelig frist. Hvis sagen kræver yderligere undersøgelse eller koordinering med en anden tilsynsmyndighed, bør den registrerede undervejs underrettes herom. For at lette indgivelsen af klager bør hver tilsynsmyndighed træffe foranstaltninger som f.eks. at tilbyde en klageformular, der også kan udfyldes elektronisk, uden at udelukke andre kommunikationsmidler.

(142) Hvis en registreret finder, at vedkommendes rettigheder i henhold til denne forordning er blevet krænket, bør den pågældende have ret til at give et organ, en organisation eller en sammenslutning, som ikke arbejder med gevinst for øje, som er etableret i overensstemmelse med en medlemsstats ret, hvis vedtægtsmæssige formål er i samfundets interesse, og som beskæftiger sig med beskyttelse af personoplysninger, bemyndigelse til på vedkommendes vegne at indgive en klage til en tilsynsmyndighed, udøve adgangen til retsmidler på vegne af vedkommende eller, hvis det er fastsat i medlemsstaternes nationale ret, udøve retten til erstatning på vegne af vedkommende. En medlemsstat kan fastsætte, at et sådant organ eller en sådan organisation eller sammenslutning skal have ret til uafhængigt af en registrerets bemyndigelse at indgive en klage i den pågældende medlemsstat og have adgang til effektive retsmidler, hvis det eller den har grund til at formode, at en registrerets rettigheder er blevet krænket som følge af behandling af personoplysninger, der overtræder denne forordning. Dette organ eller denne organisation eller sammenslutning kan ikke kræve erstatning på en registrerets vegne uafhængigt af bemyndigelse fra den registrerede.

(143) Enhver fysisk eller juridisk person har ret til at anlægge annullationssøgsmål til prøvelse af afgørelser fra Databeskyttelsesrådet ved Domstolen på de betingelser, der er fastsat i artikel 263 i TEUF. De berørte tilsynsmyndigheder, som sådanne afgørelser er rettet til, skal, hvis de ønsker at anfægte afgørelserne, anlægge søgsmål inden for to måneder efter meddelelse af afgørelserne til dem i overensstemmelse med artikel 263 i TEUF. Når en dataansvarlig, databehandler eller klager er umiddelbart og individuelt berørt af Databeskyttelsesrådets afgørelser, kan disse anlægge annullationssøgsmål til prøvelse af disse afgørelser senest to måneder efter afgørelsernes offentliggørelse på Databeskyttelsesrådets websted i overensstemmelse med artikel 263 i TEUF. Uden at dette berører denne ret i henhold til artikel 263 i TEUF, bør enhver fysisk eller juridisk person have adgang til effektive retsmidler ved den kompetente nationale domstol til prøvelse af en tilsynsmyndigheds afgørelse, som har retsvirkninger for denne person. En sådan afgørelse vedrører navnlig tilsynsmyndighedens udøvelse af undersøgelsesbeføjelser, korrigerende beføjelser og godkendelsesbeføjelser eller afslag eller afvisning af klager. Denne ret til adgang til effektive retsmidler omfatter dog ikke foranstaltninger truffet af tilsynsmyndigheder, der ikke er juridisk bindende, som f.eks. udtalelser eller rådgivning fra tilsynsmyndigheden. En sag mod en tilsynsmyndighed bør anlægges ved domstolene i den medlemsstat, hvor tilsynsmyndigheden er etableret, og bør føres i overensstemmelse med den pågældende medlemsstats retspleje. Disse domstole bør have fuld jurisdiktion, herunder jurisdiktion til at undersøge alle de faktiske og retlige omstændigheder, der er relevante for den tvist, som de får forelagt.

Hvis en klage er blevet afslået eller afvist af en tilsynsmyndighed, kan klageren anlægge sag ved domstolene i samme medlemsstat. I forbindelse med domstolskontrol vedrørende anvendelsen af denne forordning kan eller i det tilfælde, der er omhandlet i artikel 267 i TEUF, skal de nationale domstole, som anser en afgørelse om spørgsmålet for nødvendig for at afsige dom, anmode Domstolen om en præjudiciel afgørelse om fortolkning af EU-retten, herunder denne forordning. Hvis en afgørelse truffet af en tilsynsmyndighed, som gennemfører en afgørelse fra Databeskyttelsesrådet, anfægtes ved en national domstol, og gyldigheden af Databeskyttelsesrådets afgørelse er omtvistet, har den nationale domstol ikke beføjelse til at erklære Databeskyttelsesrådets afgørelse for ugyldig, men skal forelægge Domstolen spørgsmålet om gyldighed i henhold til artikel 267 i TEUF som fortolket af Domstolen, hvis den anser afgørelsen for ugyldig. En national domstol kan imidlertid ikke forelægge et spørgsmål om gyldigheden af Databeskyttelsesrådets afgørelse efter anmodning fra en fysisk eller juridisk person, der havde mulighed for at indbringe et annullationssøgsmål til prøvelse af den pågældende afgørelse, navnlig hvis personen er umiddelbart og individuelt berørt af afgørelsen, men ikke havde gjort dette inden for fristen i henhold til artikel 263 i TEUF.

(144) Hvis en domstol, for hvilken der indbringes en sag til prøvelse af en afgørelse truffet af en tilsynsmyndighed, har grund til at tro, at en sag vedrørende samme behandling, f.eks. med samme genstand for så vidt angår behandling udført af den samme dataansvarlige eller databehandler, eller som hviler på samme grundlag, anlægges ved en kompetent domstol i en anden medlemsstat, bør den kontakte den pågældende domstol for at bekræfte eksistensen af sådanne relaterede sager. Hvis der verserer relaterede sager for en domstol i en anden medlemsstat,

kan enhver anden domstol end den, ved hvilken sagen først er anlagt, udsætte sagen eller kan efter begæring fra en af parterne erklære sig inkompetent til fordel for den domstol, ved hvilken sagen først er anlagt, forudsat at denne domstol har kompetence til at behandle den pågældende sag, og forening af sådanne relaterede sager er tilladt i henhold til dens lovgivning. Sager anses for at være relaterede, når de er så snævert forbundne, at det er ønskeligt at behandle og påkende dem samtidig for at undgå risiko for uforenelige afgørelser som følge af, at de blev påkendt hver for sig.

(145) For så vidt angår sager mod en dataansvarlig eller databehandler bør sagsøger have valget mellem at indbringe sagen for domstolene i de medlemsstater, hvor den dataansvarlige eller databehandleren er etableret, eller i den medlemsstat, hvor den registrerede er bosiddende, medmindre den dataansvarlige er en offentlig myndighed i en medlemsstat og udøver offentligretlige beføjelser.

(146) Den dataansvarlige eller databehandleren bør yde erstatning for enhver skade, som en person måtte lide som følge af behandling, der overtræder denne forordning. Den dataansvarlige eller databehandleren bør være fritaget for erstatningsansvar, hvis den pågældende beviser ikke at være ansvarlig for den forvoldte skade. Begrebet »skade« bør fortolkes bredt i lyset af retspraksis ved Domstolen, således at det fuldt ud afspejler formålene for denne forordning. Dette berører ikke eventuelle erstatningskrav for skade som følge af overtrædelse af andre bestemmelser i EU-retten eller medlemsstaternes nationale ret. Behandling, der overtræder denne forordning, omfatter også behandling, der overtræder delegerede retsakter og gennemførelsesretsakter vedtaget i henhold til denne forordning og til medlemsstaternes nationale ret, der præciserer bestemmelserne i denne forordning. Registrerede bør have fuld erstatning for den skade, som de har lidt. Hvis dataansvarlige eller databehandlere er involveret i den samme behandling, bør den enkelte dataansvarlige eller databehandler hæfte for hele erstatningen. Hvis de imidlertid er inddraget i den samme retssag i overensstemmelse med medlemsstaternes nationale ret, kan erstatning fordeles i henhold til den enkelte dataansvarliges eller databehandlers ansvar for den skade, der er forvoldt af behandlingen, forudsat at der sikres fuld erstatning til den registrerede, som har lidt skaden. Enhver dataansvarlig eller databehandler, der har betalt fuld erstatning, kan efterfølgende gøre regres mod andre dataansvarlige eller databehandlere, der er involveret i samme behandling.

(147) Når denne forordning indeholder specifikke kompetenceregler, navnlig for så vidt angår sager om adgang til retsmidler, herunder erstatning, mod en dataansvarlig eller databehandler, bør de almindelige kompetenceregler i Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012 ([1]) ikke berøre anvendelsen af sådanne specifikke regler.

(148) For at styrke håndhævelsen af reglerne i denne forordning bør der pålægges sanktioner, herunder administrative bøder, for overtrædelse af denne forordning i tillæg til eller i stedet for passende foranstaltninger, som tilsynsmyndigheden har pålagt i henhold til denne forordning. I tilfælde af en mindre overtrædelse, eller hvis den bøde, der kunne blive pålagt, ville udgøre en uforholdsmæssig stor byrde for en fysisk person, kan der udstedes en irettesættelse i stedet for en bøde. Der bør dog tages behørigt hensyn til overtrædelsens karakter, alvor og varighed, overtrædelsens eventuelle forsætlige karakter, foranstaltninger, der er truffet for at begrænse den forvoldte skade, graden af ansvar eller eventuelle relevante tidligere overtrædelser, måden, hvorpå tilsynsmyndigheden fik kendskab til overtrædelsen, overholdelse af foranstaltninger truffet over for den dataansvarlige eller databehandleren, overholdelse af en adfærdskodeks samt andre skærpende eller formildende faktorer. Pålæggelse af sanktioner, herunder administrative bøder, bør være omfattet af fornødne proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og chartret, herunder effektiv retsbeskyttelse og en retfærdig procedure.

(149) Medlemsstaterne bør kunne fastsætte regler om strafferetlige sanktioner for overtrædelse af denne forordning, herunder for overtrædelse af nationale regler vedtaget i henhold til og inden for rammerne af denne forordning. Disse strafferetlige sanktioner kan også åbne mulighed for fratagelse af den opnåede fortjeneste ved overtrædelse af denne forordning. Pålæggelse af strafferetlige sanktioner for overtrædelse af sådanne nationale regler og administrative sanktioner bør dog ikke føre til et brud på ne bis in idem-princippet som fortolket af Domstolen.

(150) For at styrke og harmonisere de administrative sanktioner for overtrædelse af denne forordning bør hver tilsynsmyndighed have beføjelse til at pålægge administrative bøder. Denne forordning bør angive overtrædelser

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012 af 12. december 2012 om retternes kompetence og om anerkendelse og fuldbyrdelse af retsafgørelser på det civil- og handelsretlige område (EUT L 351 af 20.12.2012, s. 1).

og maksimumsbeløb og kriterier for fastsættelse af de tilknyttede administrative bøder, der bør bestemmes af den kompetente tilsynsmyndighed i hvert enkelt tilfælde under hensyntagen til alle relevante omstændigheder i den specifikke situation og med behørig hensyntagen til karakteren, alvoren og varigheden af overtrædelsen og dens konsekvenser og de foranstaltninger, der er truffet for at sikre overholdelse af forpligtelserne i henhold til denne forordning og for at forebygge eller begrænse følgerne af overtrædelsen. Når en virksomhed pålægges administrative bøder, forstås en virksomhed i denne forbindelse som en virksomhed som omhandlet i artikel 101 og 102 i TEUF. Når personer, der ikke er en virksomhed, pålægges administrative bøder, bør tilsynsmyndigheden i forbindelse med fastsættelsen af bødestørrelsen tage hensyn til det generelle indkomstniveau i den pågældende medlemsstat og personens økonomiske situation. Sammenhængsmekanismen kan også anvendes til at fremme konsekvent anvendelse af administrative bøder. Det bør være op til medlemsstaterne at bestemme, om og i hvilket omfang de offentlige myndigheder bør kunne pålægges administrative bøder. Pålæggelse af en administrativ bøde eller udstedelse af en advarsel berører ikke anvendelsen af tilsynsmyndighedernes øvrige beføjelser eller andre sanktioner i henhold til denne forordning.

(151) Retssystemerne i Danmark og Estland giver ikke mulighed for administrative bøder som fastsat i denne forordning. Reglerne om administrative bøder kan i Danmark anvendes ved, at bøder pålægges af de kompetente nationale domstole som en strafferetlig sanktion, og i Estland ved, at bøder pålægges af tilsynsmyndigheden inden for rammerne af en forseelsesprocedure, forudsat at en sådan anvendelse af reglerne i disse medlemsstater har en virkning, der svarer til virkningen af administrative bøder, som tilsynsmyndighederne pålægger. De kompetente nationale domstole bør derfor tage hensyn til en anbefaling fra den tilsynsmyndighed, der har taget skridt til en bøde. De pålagte bøder bør under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

(152) Når denne forordning ikke harmoniserer administrative sanktioner eller om nødvendigt i andre tilfælde, f.eks. i tilfælde af alvorlige overtrædelser af denne forordning, bør medlemsstaterne indføre en ordning, der giver mulighed for at pålægge sanktioner, som er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning. Sanktionernes art, strafferetlig eller administrativ, bør fastsættes i medlemsstaternes nationale ret.

(153) Medlemsstatslovgivningen bør forene reglerne om ytrings- og informationsfrihed, herunder i forbindelse med journalistisk, akademisk, kunstnerisk og/eller litterær virksomhed, med retten til beskyttelse af personoplysninger i henhold til denne forordning. Der bør fastsættes undtagelser eller fravigelser fra visse bestemmelser i denne forordning for behandling af personoplysninger, der udelukkende finder sted i journalistisk øjemed eller med henblik på akademisk, kunstnerisk eller litterær virksomhed, hvis det er nødvendigt for at forene retten til beskyttelse af personoplysninger med retten til ytrings- og informationsfrihed som garanteret ved artikel 11 i chartret. Dette bør navnlig gælde for behandlingen af personoplysninger på det audiovisuelle område og i nyhedsarkiver og pressebiblioteker. Medlemsstaterne bør derfor vedtage lovgivningsmæssige foranstaltninger, der fastlægger undtagelser og fravigelser, som er nødvendige af hensyn til balancen mellem disse grundlæggende rettigheder. Medlemsstaterne bør vedtage sådanne undtagelser og fravigelser vedrørende generelle principper, den registreredes rettigheder, den dataansvarlige og databehandleren, overførsel af personoplysninger til tredjelande eller internationale organisationer, de uafhængige tilsynsmyndigheder, samarbejde og sammenhæng samt specifikke databehandlingssituationer. Hvis disse undtagelser eller fravigelser varierer fra en medlemsstat til en anden, bør den nationale ret i den medlemsstat, som den dataansvarlige er underlagt, finde anvendelse. For at tage hensyn til betydningen af retten til ytringsfrihed i ethvert demokratisk samfund er det nødvendigt at tolke begreber vedrørende denne frihed, f.eks. journalistik, bredt.

(154) Denne forordning giver mulighed for, at der ved anvendelsen af denne forordning, kan tages hensyn til princippet om aktindsigt i officielle dokumenter. Aktindsigt i officielle dokumenter kan anses for at være i samfundets interesse. Personoplysninger i dokumenter, der opbevares af en offentlig myndighed eller et offentligt organ, bør kunne offentliggøres af denne myndighed eller dette organ, hvis dette er fastsat i EU-retten eller medlemsstaternes nationale ret, som den offentlige myndighed eller det offentlige organ er underlagt. Sådanne regler bør forene aktindsigt i officielle dokumenter og videreanvendelse af den offentlige sektors information med retten til beskyttelse af personoplysninger og kan derfor indeholde den nødvendige forening med retten til beskyttelse af personoplysninger i henhold til denne forordning. Offentlige myndigheder og organer bør i denne sammenhæng omfatte alle myndigheder eller andre organer, der er omfattet af medlemsstaternes nationale ret om aktindsigt. Europa-Parlamentets og Rådets direktiv 2003/98/EF ([1]) opretholder og griber på ingen måde ind i beskyttelsesniveauet for fysiske personer med hensyn til behandling af personoplysninger i henhold til EU-retten og

([1]) Europa-Parlamentets og Rådets direktiv 2003/98/EF af 17. november 2003 om videreanvendelse af den offentlige sektors informationer (EUT L 345 af 31.12.2003, s. 90).

medlemsstaternes nationale ret, og det ændrer navnlig ikke de forpligtelser og rettigheder, der er fastsat i denne forordning. Dette direktiv bør navnlig ikke gælde for dokumenter, hvortil adgang er udelukket eller begrænset i henhold til aktindsigtsordningerne under henvisning til beskyttelse af personoplysninger, og dele af dokumenter, der i henhold til disse ordninger er adgang til, og som indeholder personoplysninger, hvis videreanvendelse ifølge lovgivningen er uforenelig med lovgivningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

(155) 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, og i forbindelse med ansættelse, ansættelseskontrakter, herunder godtgørelse for forpligtelser fastlagt ved lov eller kollektive overenskomster, ledelse, planlægning og tilrettelæggelse af arbejdet, ligestilling og mangfoldighed på arbejdspladsen, sikkerhed og sundhed på arbejdspladsen, individuel eller kollektiv udøvelse og nydelse af rettigheder og fordele i forbindelse med ansættelse samt ophør af ansættelsesforhold.

(156) 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 registrerede rettigheder og frihedsrettigheder i henhold til denne forordning. Disse garantier bør sikre, at der er truffet tekniske og organisatoriske foranstaltninger for især at sikre princippet om dataminimering. 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). Medlemsstaterne bør sikre de fornødne garantier for behandling af personoplysninger til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål. Medlemsstaterne bør have tilladelse til på særlige betingelser og med de fornødne garantier for de registrerede at fastsætte præciseringer af og undtagelser med hensyn til oplysningskravene og retten til berigtigelse eller sletning af personoplysninger, retten til at blive glemt, retten til begrænsning af behandling, retten til dataportabilitet og retten til indsigelse i forbindelse med behandling af personoplysninger til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål. De pågældende betingelser og garantier kan indebære specifikke procedurer for registreredes udøvelse af rettigheder, hvis dette er relevant i lyset af de formål, der tilstræbes med den specifikke behandling, foruden tekniske og organisatoriske foranstaltninger med henblik på at minimere behandlingen af personoplysninger i medfør af proportionalitetsprincippet og nødvendighedsprincippet. Behandling af personoplysninger til videnskabelige formål bør også overholde anden relevant lovgivning, f.eks. om kliniske forsøg.

(157) Ved at sammenstille oplysninger fra registre kan forskere opnå ny viden af stor værdi for så vidt angår udbredte sygdomstilstande såsom hjerte-kar-sygdomme, kræft og depression. På basis af registre kan forskningsresultater styrkes, da de bygger på en større befolkningsgruppe. Inden for samfundsvidenskab gør forskning på basis af registre det muligt for forskere at opnå afgørende viden om langtidssammenhæng mellem en række sociale forhold, f.eks. arbejdsløshed og uddannelse, med andre livsvilkår. Forskningsresultater, der opnås gennem registre, leverer solid viden af høj kvalitet, som kan danne grundlag for udformning og gennemførelse af videnbaseret politik, forbedre livskvaliteten for mange mennesker og øge effektiviteten af de sociale tjenester. For at fremme videnskabelig forskning kan personoplysninger behandles til videnskabelige forskningsformål under iagttagelse af passende betingelser og garantier i EU-retten eller medlemsstaternes nationale ret.

(158) Når personoplysninger behandles til arkivformål, bør denne forordning også gælde for den pågældende behandling, idet denne forordning dog ikke bør finde anvendelse på afdøde personer. Offentlige myndigheder eller offentlige eller private organer, der opbevarer fortegnelser af samfundsinteresse, bør være tjenester, der i henhold til EU-retten eller medlemsstaternes nationale ret har retlig forpligtelse til at indhente, bevare, vurdere, ordne, beskrive, udlevere, fremme, formidle og give adgang til fortegnelser af blivende værdi i samfundets interesse. Medlemsstaterne bør også have tilladelse til at fastsætte, at personoplysninger kan viderebehandles til arkivformål, f.eks. for at tilvejebringe specifikke oplysninger om politisk adfærd under tidligere totalitære regimer, folkedrab, forbrydelser mod menneskeheden, navnlig holocaust, eller krigsforbrydelser.

(159) 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.

(160) Når personoplysninger behandles til historiske forskningsformål, bør denne forordning også gælde for denne behandling. Dette bør også omfatte historisk forskning og forskning i genealogisk øjemed, idet denne forordning dog ikke bør gælde for afdøde personer.

(161) For så vidt angår samtykke til deltagelse i videnskabelige forskningsaktiviteter i forbindelse med kliniske forsøg bør de relevante bestemmelser i Europa-Parlamentets og Rådets forordning (EU) nr. 536/2014 ([1]) finde anvendelse.

(162) Når personoplysninger behandles til statistiske formål, bør denne forordning finde anvendelse på denne behandling. EU-retten eller medlemsstaternes nationale ret bør inden for rammerne af denne forordning 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. Disse statistiske resultater kan videreanvendes til forskellige formål, herunder videnskabelige forskningsformål. Det statistiske formål indebærer, at resultatet af behandling til statistiske formål ikke er personoplysninger, men aggregerede data, og at dette resultat eller personoplysningerne ikke anvendes til støtte for foranstaltninger eller afgørelser, der vedrører bestemte fysiske personer.

(163) De fortrolige oplysninger, som Unionen og de nationale statistikmyndigheder indsamler til udarbejdelse af officielle europæiske og officielle nationale statistikker, bør beskyttes. Europæiske statistikker bør udvikles, udarbejdes og formidles i overensstemmelse med de statistiske principper, der er beskrevet i artikel 338, stk. 2, i TEUF, mens nationale statistikker også bør overholde medlemsstaternes nationale ret. Europa-Parlamentets og Rådets forordning (EF) nr. 223/2009 ([2]) indeholder yderligere præciseringer om statistisk fortrolighed for europæiske statistikker.

(164) Hvad angår tilsynsmyndighedernes beføjelser til af den dataansvarlige eller databehandleren at få indsigt i personoplysninger og adgang til den pågældendes lokaler kan medlemsstaterne inden for rammerne af denne forordning ved lov vedtage specifikke regler med det formål at sikre faglig eller anden tilsvarende tavshedspligt, for så vidt det er nødvendigt for at forene retten til beskyttelse af personoplysninger med tavshedspligt. Dette berører ikke medlemsstaternes eksisterende forpligtelser til at vedtage regler om tavshedspligt, hvis det kræves i EU-retten.

(165) Denne forordning respekterer og anfægter ikke den status i henhold til eksisterende forfatningsretlige bestemmelser, som kirker og religiøse sammenslutninger eller samfund har i medlemsstaterne, jf. artikel 17 i TEUF.

(166) For at opfylde denne forordnings målsætninger, dvs. at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger, og for at sikre fri udveksling af personoplysninger i Unionen bør beføjelsen til at vedtage retsakter i henhold til artikel 290 i TEUF delegeres til

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 536/2014 af 16. april 2014 om kliniske forsøg med humanmedicinske lægemidler og om ophævelse af direktiv 2001/20/EF (EUT L 158 af 27.5.2014, s. 1).

([2]) Europa-Parlamentets og Rådets forordning (EF) nr. 223/2009 af 11. marts 2009 om europæiske statistikker og om ophævelse af forordning (EF, Euratom) nr. 1101/2008 om fremsendelse af fortrolige statistiske oplysninger til De Europæiske Fællesskabers Statistiske Kontor, Rådets forordning (EF) nr. 322/97 om EF-statistikker og Rådets afgørelse 89/382/EØF, Euratom om nedsættelse af et udvalg for De Europæiske Fællesskabers statistiske program (EUT L 87 af 31.3.2009, s. 164).

Kommissionen. Der bør navnlig 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 er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau. Kommissionen bør sikre samtidig, rettidig og hensigtsmæssig fremsendelse af relevante dokumenter til Europa-Parlamentet og til Rådet, når den forbereder og udarbejder delegerede retsakter.

(167) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser, når dette er fastsat i denne forordning. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011. I den forbindelse bør Kommissionen overveje specifikke foranstaltninger for mikrovirksomheder og små og mellemstore virksomheder.

(168) Undersøgelsesproceduren bør anvendes til vedtagelse af gennemførelsesretsakter om standardkontraktbestemmelser mellem dataansvarlige og databehandlere og mellem databehandlere indbyrdes, adfærdskodekser, tekniske standarder og certificeringsmekanismer, tilstrækkeligt databeskyttelsesniveau, der sikres af et tredjeland, et område eller en specifik sektor i dette tredjeland, eller en international organisation, standardbestemmelser om databeskyttelse, formater og procedurer for elektronisk udveksling af oplysninger mellem dataansvarlige, databehandlere og tilsynsmyndigheder for bindende virksomhedsregler, gensidig bistand og ordninger for elektronisk udveksling af oplysninger mellem tilsynsmyndigheder og mellem tilsynsmyndigheder og Databeskyttelsesrådet.

(169) Kommissionen bør vedtage gennemførelsesretsakter, der finder anvendelse straks, når foreliggende dokumentation viser, at et tredjeland, et område eller en specifik sektor i dette tredjeland, eller en international organisation ikke sikrer et tilstrækkeligt beskyttelsesniveau, og når det er påkrævet i særlig hastende tilfælde.

(170) Målet for denne forordning, nemlig at sikre et ensartet niveau for beskyttelse af fysiske personer og fri udveksling af oplysninger i Unionen, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union (TEU). I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå dette mål.

(171) Direktiv 95/46/EF bør ophæves ved denne forordning. Behandling, der allerede er indledt på datoen for denne forordnings anvendelse, bør bringes i overensstemmelse med forordningen senest to år efter ikrafttrædelsen heraf. Når behandling er baseret på samtykke i henhold til direktiv 95/46/EF, er det ikke nødvendigt, at den registrerede på ny giver sit samtykke, 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 denne forordnings anvendelsesdato. Kommissionsafgørelser og -beslutninger, der er vedtaget i henhold til direktiv 95/46/EF, og tilsynsmyndigheders godkendelser baseret på direktiv 95/46/EF bør fortsat gælde, indtil de ændres, erstattes eller ophæves.

(172) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001 og afgav en udtalelse den 7. marts 2012 ([1]).

(173) Denne forordning bør gælde for alle forhold vedrørende beskyttelse af grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger, som ikke er underlagt specifikke forpligtelser med samme formål som fastsat i Europa-Parlamentets og Rådets direktiv 2002/58/EF ([2]), herunder den dataansvarliges forpligtelser og fysiske personers rettigheder. For at afklare forholdet mellem denne forordning og direktiv 2002/58/EF bør nævnte direktiv ændres i overensstemmelse hermed. Når denne forordning er vedtaget, bør direktiv 2002/58/EF revideres, navnlig for at sikre forenelighed med denne forordning —

([1]) EUT C 192 af 30.6.2012, s. 7.
([2]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (EFT L 201 af 31.7.2002, s. 37).

HAR VEDTAGET DENNE FORORDNING

KAPITEL I

Generelle bestemmelser

Artikel 1

Genstand og formål

1. I denne forordning fastsættes regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og regler om fri udveksling af personoplysninger.

2. Denne forordning beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger.

3. Den frie udveksling af personoplysninger i Unionen må hverken indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

Artikel 2

Materielt anvendelsesområde

1. Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

2. Denne forordning gælder ikke for behandling af personoplysninger:

a) under udøvelse af aktiviteter, der falder uden for EU-retten

b) som foretages af medlemsstaterne, når de udfører aktiviteter, der falder inden for rammerne af afsnit V, kapitel 2, i TEU

c) som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter

d) 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.

3. Forordning (EF) nr. 45/2001 finder anvendelse på behandling af personoplysninger, som Unionens institutioner, organer, kontorer og agenturer foretager. Forordning (EF) nr. 45/2001 og andre EU-retsakter, der finder anvendelse på sådan behandling af personoplysninger, tilpasses til principperne og bestemmelserne i nærværende forordning i overensstemmelse med artikel 98.

4. Denne forordning berører ikke anvendelsen af direktiv 2000/31/EF, navnlig reglerne om formidleransvar for tjenesteydere, der er fastsat i artikel 12-15 i nævnte direktiv.

Artikel 3

Territorialt anvendelsesområde

1. Denne forordning finder anvendelse på behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i Unionen, uanset om behandlingen finder sted i Unionen eller ej.

2. Denne forordning 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:

a) udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet, eller

b) overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Unionen.

3. Denne forordning anvendes 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.

Artikel 4

Definitioner

I denne forordning forstås ved:

1) »personoplysninger«: 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

2) »behandling«: 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

3) »begrænsning af behandling«: mærkning af opbevarede personoplysninger med den hensigt at begrænse fremtidig behandling af disse oplysninger

4) »profilering«: 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

5) »pseudonymisering«: 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

6) »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

7) »dataansvarlig«: 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

8) »databehandler«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne

9) »modtager«: 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; de offentlige myndigheders behandling af disse oplysninger skal overholde de gældende databeskyttelsesregler afhængigt af formålet med behandlingen

10) »tredjemand«: 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

11) »samtykke« fra den registrerede: 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

12) »brud på persondatasikkerheden«: 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

13) »genetiske data«: 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

14) »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

15) »helbredsoplysninger«: personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand

16) »hovedvirksomhed«:

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

17) »repræsentant«: 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

18) »foretagende«: en fysisk eller juridisk person, som udøver økonomisk aktivitet, uanset dens retlige status, herunder partnerskaber eller sammenslutninger, der regelmæssigt udøver økonomisk aktivitet

19) »koncern«: en virksomhed, der udøver kontrol, og de af denne kontrollerede virksomheder

20) »bindende virksomhedsregler«: 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

21) »tilsynsmyndighed«: en uafhængig offentlig myndighed, der er etableret i en medlemsstat i henhold til artikel 51

22) »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

23) »grænseoverskridende behandling«:

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

24) »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

25) »informationssamfundstjeneste«: en tjeneste som defineret i artikel 1, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 ([1])

26) »international organisation«: 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.

KAPITEL II

Principper

Artikel 5

Principper for behandling af personoplysninger

1. Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)

b) 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«)

c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)

d) 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«)

([1]) 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).

e) 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 (»opbevaringsbegrænsning«)

f) 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 (»integritet og fortrolighed«).

2. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).

Artikel 6

Lovlig behandling

1. Behandling er kun lovlig, hvis og i det omfang mindst ét af følgende forhold gør sig gældende:

a) Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.

b) 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.

c) Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.

d) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.

e) 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.

f) 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.

Første afsnit, litra f), gælder ikke for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

2. 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.

3. Grundlaget for behandling i henhold til stk. 1, litra c) og e), skal fremgå af:

a) EU-retten, eller

b) 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. 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.

4. Når behandling til et andet formål end det, som personoplysningerne er indsamlet til, ikke er baseret på den registreredes samtykke eller EU-retten eller medlemsstaternes nationale ret, som udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1, tager den dataansvarlige, for at afgøre, om behandling til et andet formål er forenelig med det formål, som personoplysningerne oprindelig blev indsamlet til, bl.a. hensyn til følgende:

a) enhver forbindelse mellem det formål, som personoplysningerne er indsamlet til, og formålet med den påtænkte viderebehandling

b) den sammenhæng, hvori personoplysningerne er blevet indsamlet, navnlig med hensyn til forholdet mellem den registrerede og den dataansvarlige

c) personoplysningernes art, navnlig om særlige kategorier af personoplysninger behandles, jf. artikel 9, eller om personoplysninger vedrørende straffedomme og lovovertrædelser behandles, jf. artikel 10

d) den påtænkte viderebehandlings mulige konsekvenser for de registrerede

e) tilstedeværelse af fornødne garantier, som kan omfatte kryptering eller pseudonymisering.

Artikel 7

Betingelser for samtykke

1. Hvis behandling er baseret på samtykke, skal den dataansvarlige kunne påvise, at den registrerede har givet samtykke til behandling af sine personoplysninger.

2. 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.

3. Den registrerede har til enhver tid 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.

4. 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.

Artikel 8

Betingelser for et barns samtykke i forbindelse med informationssamfundstjenester

1. 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.

2. 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.

3. Stk. 1 berører ikke medlemsstaternes generelle aftaleret, som f.eks. bestemmelser om gyldighed, indgåelse eller virkning af en kontrakt, når der er tale om et barn.

Artikel 9

Behandling af særlige kategorier af personoplysninger

1. 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.

2. Stk. 1 finder ikke anvendelse, hvis et af følgende forhold gør sig gældende:

a) 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.

b) 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.

c) 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.

d) 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.

e) Behandling vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede.

f) Behandling er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol.

g) 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.

h) 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 stk. 3.

i) 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.

j) 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.

3. Personoplysninger som omhandlet i stk. 1 kan 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.

4. Medlemsstaterne kan opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger.

Artikel 10

Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser

Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på grundlag af artikel 6, stk. 1, må 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. Ethvert omfattende register over straffedomme må kun føres under kontrol af en offentlig myndighed.

Artikel 11

Behandling, der ikke kræver identifikation

1. 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, indhente eller behandle yderligere oplysninger for at kunne identificere den registrerede alene med det formål at overholde denne forordning.

2. Hvis den dataansvarlige i tilfælde, der er omhandlet i denne artikels 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 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.

KAPITEL III

Den registreredes rettigheder

Afdeling 1

Gennemsigtighed og nærmere regler

Artikel 12

Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder

1. Den dataansvarlige træffer 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 oplysningerne gives mundtligt, forudsat at den registreredes identitet godtgøres med andre midler.

2. Den dataansvarlige letter udøvelsen af den registreredes rettigheder i henhold til artikel 15-22. 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.

3. Den dataansvarlige oplyser uden unødig forsinkelse og i alle tilfælde senest en måned efter modtagelsen af anmodningen 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.

4. 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 en klage til en tilsynsmyndighed og indbringe sagen for en retsinstans.

5. 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.

Bevisbyrden for, at anmodningen er åbenbart grundløs eller overdreven, påhviler den dataansvarlige.

6. Uden at det berører artikel 11 kan den dataansvarlige, hvis der hersker rimelig tvivl om identiteten af den fysiske person, der fremsætter en anmodning som omhandlet i artikel 15-21, anmode om yderligere oplysninger, der er nødvendige for at bekræfte den registreredes identitet.

7. De oplysninger, der skal gives til 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.

8. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 92 med henblik på at fastlægge de oplysninger, der skal fremgå af ikoner, og procedurerne for tilvejebringelse af standardiserede ikoner.

Afdeling 2

Oplysning og indsigt i personoplysninger

Artikel 13

Oplysningspligt ved indsamling af personoplysninger hos den registrerede

1. Hvis personoplysninger om en registreret indsamles hos den registrerede, giver den dataansvarlige på det tidspunkt, hvor personoplysningerne indsamles, den registrerede alle følgende oplysninger:

a) identitet på og kontaktoplysninger for den dataansvarlige og dennes eventuelle repræsentant

b) kontaktoplysninger for en eventuel databeskyttelsesrådgiver

c) formålene med den behandling, som personoplysningerne skal bruges til, og retsgrundlaget for behandlingen

d) de legitime interesser, som forfølges af den dataansvarlige eller en tredjemand, hvis behandlingen er baseret på artikel 6, stk. 1, litra f)

e) eventuelle modtagere eller kategorier af modtagere af personoplysningerne

f) hvor det er relevant, 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, andet afsnit, litra h), henvisning til de fornødne eller passende garantier, og hvordan der kan fås en kopi heraf, eller hvor de er blevet gjort tilgængelige.

2. Ud over de oplysninger, der er omhandlet i stk. 1, giver den dataansvarlige på det tidspunkt, hvor personoplysningerne indsamles, den registrerede følgende yderligere oplysninger, der er nødvendige for at sikre en rimelig og gennemsigtig behandling:

a) det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum

b) retten til at anmode den dataansvarlige 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

c) når behandling er baseret på artikel 6, stk. 1, litra a), eller artikel 9, stk. 2, litra a), retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf

d) retten til at indgive en klage til en tilsynsmyndighed

e) 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 personoplysningerne og de eventuelle konsekvenser af ikke at give sådanne oplysninger

f) 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.

3. 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.

4. Stk. 1, 2 og 3 finder ikke anvendelse, hvis og i det omfang den registrerede allerede er bekendt med oplysningerne.

Artikel 14

Oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede

1. Hvis personoplysningerne ikke er indsamlet hos den registrerede, giver den dataansvarlige den registrerede følgende oplysninger:

a) identitet på og kontaktoplysninger for den dataansvarlige og dennes eventuelle repræsentant

b) kontaktoplysninger for en eventuel databeskyttelsesrådgiver

c) formålene med den behandling, som personoplysningerne skal bruges til, samt retsgrundlaget for behandlingen

d) de berørte kategorier af personoplysninger

e) eventuelle modtagere eller kategorier af modtagere af personoplysningerne

f) hvor det er relevant, at den dataansvarlige agter at overføre personoplysninger til en modtager i 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, andet afsnit, litra h), henvisning til de fornødne eller passende garantier, og hvordan der kan fås en kopi heraf, eller hvor de er blevet gjort tilgængelige.

2. Ud over de oplysninger, der er omhandlet i stk. 1, giver den dataansvarlige den registrerede følgende oplysninger, der er nødvendige for at sikre en rimelig og gennemsigtig behandling for så vidt angår den registrerede:

a) det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum

b) de legitime interesser, som forfølges af den dataansvarlige eller en tredjemand, hvis behandlingen er baseret på artikel 6, stk. 1, litra f)

c) retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede og til at gøre indsigelse mod behandling samt retten til dataportabilitet

d) når behandling er baseret på artikel 6, stk. 1, litra a), eller artikel 9, stk. 2, litra a), retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf

e) retten til at indgive en klage til en tilsynsmyndighed

f) hvilken kilde personoplysningerne hidrører fra, og eventuelt hvorvidt de stammer fra offentligt tilgængelige kilder

g) 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.

3. Den dataansvarlige giver de oplysninger, der er omhandlet i stk. 1 og 2:

a) inden for en rimelig frist efter indsamlingen af personoplysningerne, men senest inden for en måned under hensyn til de specifikke forhold, som personoplysningerne er behandlet under,

b) hvis personoplysningerne skal bruges til at kommunikere med den registrerede, senest på tidspunktet for den første kommunikation med den registrerede, eller

c) hvis personoplysningerne er bestemt til videregivelse til en anden modtager, senest når personoplysningerne videregives første gang.

4. 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 samt andre relevante yderligere oplysninger, jf. stk. 2.

5. Stk. 1-4 finder ikke anvendelse, hvis og i det omfang:

a) den registrerede allerede er bekendt med oplysningerne

b) meddelelse af sådanne oplysninger viser sig umulig eller vil kræve en 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. I sådanne tilfælde træffer den dataansvarlige passende foranstaltninger for at beskytte den registreredes rettigheder og frihedsrettigheder samt legitime interesser, herunder ved at gøre oplysningerne offentligt tilgængelige

c) 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, eller

d) personoplysningerne skal forblive fortrolige som følge af tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret, herunder lovbestemt tavshedspligt.

Artikel 15

Den registreredes indsigtsret

1. 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

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

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.

2. 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.

3. 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.

4. Retten til at modtage en kopi som omhandlet i stk. 3 må ikke krænke andres rettigheder og frihedsrettigheder.

Afdeling 3

Berigtigelse og sletning

Artikel 16

Ret til berigtigelse

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.

Artikel 17

Ret til sletning (»retten til at blive glemt«)

1. 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 et 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.

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.

2. Hvis den dataansvarlige har offentliggjort personoplysningerne og i henhold til stk. 1 er forpligtet til at slette personoplysningerne, træffer den dataansvarlige under hensyntagen til den teknologi, der er tilgængelig, og omkostningerne ved implementeringen, rimelige foranstaltninger, herunder tekniske foranstaltninger, for at underrette de dataansvarlige, som behandler personoplysningerne, om, at den registrerede har anmodet disse dataansvarlige om at slette alle link til eller kopier eller gengivelser af de pågældende personoplysninger.

3. Stk. 1 og 2 finder ikke anvendelse, i det omfang denne behandling er nødvendig:

a) for at udøve retten til ytrings- og informationsfrihed

b) 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

c) af hensyn til samfundsinteresser på folkesundhedsområdet i overensstemmelse med artikel 9, stk. 2, litra h) og i), samt artikel 9, stk. 3

d) til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, i det omfang den rettighed, der er omhandlet i stk. 1, sandsynligvis vil gøre det umuligt eller i alvorlig grad hindre opfyldelse af denne behandling, eller

e) for, at retskrav kan fastlægges, gøres gældende eller forsvares.

Artikel 18

Ret til begrænsning af behandling

1. 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 anvendelse 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.

2. Hvis behandling er blevet begrænset i medfør af stk. 1, må sådanne personoplysninger, bortset fra opbevaring, kun 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 eller af hensyn til Unionens eller en medlemsstats vigtige samfundsinteresser.

3. En registreret, der har opnået begrænsning af behandling i medfør af stk. 1, underrettes af den dataansvarlige, inden begrænsningen af behandlingen ophæves.

Artikel 19

Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

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.

Artikel 20

Ret til dataportabilitet

1. 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.

2. 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.

3. Udøvelsen af den ret, der er omhandlet i denne artikels stk. 1, berører ikke artikel 17. Den nævnte ret finder ikke anvendelse på behandling, der er nødvendig for udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

4. Den ret, der er omhandlet i stk. 1, må ikke krænke andres rettigheder eller frihedsrettigheder.

Afdeling 4

Ret til indsigelse og automatiske individuelle afgørelser

Artikel 21

Ret til indsigelse

1. Den registrerede har til enhver tid 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.

2. 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.

3. Hvis den registrerede gør indsigelse mod behandling med henblik på direkte markedsføring, må personoplysningerne ikke længere behandles til dette formål.

4. 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.

5. 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.

6. 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.

Artikel 22

Automatiske individuelle afgørelser, herunder profilering

1. 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.

2. Stk. 1 finder ikke anvendelse, hvis afgørelsen:

a) er nødvendig for indgåelse eller opfyldelse af en kontrakt mellem den registrerede og en dataansvarlig

b) 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 eller

c) er baseret på den registreredes udtrykkelige samtykke.

3. I de tilfælde, der er omhandlet i stk. 2, litra a) og 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.

4. De afgørelser, der er omhandlet i stk. 2, må ikke 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.

Afdeling 5

Begrænsninger

Artikel 23

Begrænsninger

1. EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige eller databehandleren er underlagt, kan ved lovgivningsmæssige foranstaltninger 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.

2. 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.

KAPITEL IV

Dataansvarlig og databehandler

Afdeling 1

Generelle forpligtelser

Artikel 24

Den dataansvarliges ansvar

1. Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

2. Hvis det står i rimeligt forhold til behandlingsaktiviteter, skal de foranstaltninger, der er omhandlet i stk. 1, omfatte den dataansvarliges implementering af passende databeskyttelsespolitikker.

3. Overholdelse af godkendte adfærdskodekser som omhandlet i artikel 40 eller godkendte certificeringsmekanismer som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af den dataansvarliges forpligtelser.

Artikel 25

Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

1. 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, gennemfører den dataansvarlige både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, såsom dataminimering, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder.

2. Den dataansvarlige gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles. Denne forpligtelse gælder den mængde personoplysninger, der indsamles, og omfanget af deres behandling samt deres opbevaringsperiode og tilgængelighed. Sådanne foranstaltninger skal navnlig gennem standardindstillinger sikre, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.

3. En godkendt certificeringsmekanisme i medfør af artikel 42 kan blive brugt som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1 og 2.

Artikel 26

Fælles dataansvarlige

1. Hvis to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til behandling, er de fælles dataansvarlige. De fastlægger på en gennemsigtig måde deres respektive ansvar for overholdelse af forpligtelserne i henhold til denne forordning, navnlig hvad angår udøvelse af den registreredes rettigheder og deres respektive forpligtelser til at fremlægge de oplysninger, der er omhandlet i artikel 13 og 14, ved hjælp af en ordning mellem dem, medmindre og i det omfang de dataansvarliges respektive ansvar er fastlagt i EU-ret eller medlemsstaternes nationale ret, som de dataansvarlige er underlagt. I ordningen kan der udpeges et kontaktpunkt for registrerede.

2. Ordningen, der er omhandlet i stk. 1, skal på behørig vis afspejle de fælles dataansvarliges respektive roller og forhold til de registrerede. Det væsentligste indhold af ordningen skal gøres tilgængeligt for de registrerede.

3. Uanset udformningen af den ordning, der er omhandlet i stk. 1, kan den registrerede udøve sine rettigheder i medfør af denne forordning med hensyn til og over for den enkelte dataansvarlige.

Artikel 27

Repræsentanter for dataansvarlige og databehandlere, der ikke er etableret i Unionen

1. Hvis artikel 3, stk. 2, finder anvendelse, udpeger den dataansvarlige eller databehandleren skriftligt en repræsentant i Unionen.

2. Forpligtelsen fastsat i denne artikels stk. 1 gælder ikke for:

a) behandling, der er lejlighedsvis, som ikke i stort omfang omfatter behandling af særlige kategorier af oplysninger, jf. artikel 9, stk. 1, eller behandling af personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10, og som sandsynligvis ikke indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder under hensyntagen til behandlingens karakter, sammenhæng, omfang og formål, eller

b) offentlige myndigheder eller organer.

3. Repræsentanten skal være etableret i en af de medlemsstater, hvor de registrerede, hvis personoplysninger behandles i forbindelse med udbud af varer eller tjenesteydelser til dem, eller hvis adfærd overvåges, er.

4. Repræsentanten bemyndiges af den dataansvarlige eller databehandleren til at modtage henvendelser ud over eller i stedet for den dataansvarlige eller databehandleren, navnlig fra tilsynsmyndigheder og registrerede, i forbindelse med alle spørgsmål vedrørende behandling med henblik på at sikre overholdelse af denne forordning.

5. Den dataansvarliges eller databehandlerens udpegning af en repræsentant berører ikke eventuelle retlige skridt mod den dataansvarlige eller databehandleren selv.

Artikel 28

Databehandler

1. 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.

2. Databehandleren må ikke gøre brug af en anden databehandler 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 andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

3. 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. Denne kontrakt eller dette andet retlige dokument fastsætter navnlig, at databehandleren:

a) 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

b) sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt

c) iværksætter alle foranstaltninger, som kræves i henhold til artikel 32

d) opfylder de betingelser, der er omhandlet i stk. 2 og 4, for at gøre brug af en anden databehandler

e) 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

f) bistår 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

g) efter den dataansvarliges valg sletter eller tilbageleverer 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

h) stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i denne artikel, 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.

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.

4. Gør en databehandler brug af en anden databehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, pålægges denne anden databehandler 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, hvorved der navnlig stilles de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i denne forordning. Hvis denne anden databehandler ikke opfylder sine databeskyttelsesforpligtelser, forbliver den oprindelige databehandler fuldt ansvarlig over for den dataansvarlige for opfyldelsen af denne anden databehandlers forpligtelser.

5. 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.

6. Uden at det berører en individuel kontrakt mellem den dataansvarlige og databehandleren, kan kontrakten eller det andet retlige dokument, der er omhandlet i denne artikels stk. 3 og 4, helt eller delvis baseres på de standardkontraktbestemmelser, der er anført i denne artikels 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.

7. Kommissionen kan fastsætte standardkontraktbestemmelser i de tilfælde, der er omhandlet i denne artikels stk. 3 og 4, og i overensstemmelse med undersøgelsesproceduren, der er omhandlet i artikel 93, stk. 2.

8. En tilsynsmyndighed kan vedtage standardkontraktbestemmelser i de tilfælde, der er omhandlet i denne artikels stk. 3 og 4, og i overensstemmelse med sammenhængsmekanismen, der er omhandlet i artikel 63.

9. Kontrakten eller det andet retlige dokument, der er omhandlet i stk. 3 og 4, skal foreligge skriftligt, herunder elektronisk.

10. Hvis 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.

Artikel 29

Behandling, der udføres for den dataansvarlige eller databehandleren

Databehandleren og enhver, der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, behandler kun disse oplysninger efter instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

Artikel 30

Fortegnelser over behandlingsaktiviteter

1. Hver dataansvarlig og hvis det er relevant, den dataansvarliges repræsentant fører fortegnelser over behandlingsaktiviteter under deres ansvar. Disse fortegnelser skal omfatte alle af følgende oplysninger:

a) navn på og kontaktoplysninger for den dataansvarlige og, hvis det er relevant, den fælles dataansvarlige, den dataansvarliges repræsentant og databeskyttelsesrådgiveren

b) formålene med behandlingen

c) en beskrivelse af kategorierne af registrerede og kategorierne af personoplysninger

d) de kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, herunder modtagere i tredjelande eller internationale organisationer

e) hvor det er relevant, 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

f) hvis det er muligt, de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger

g) hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1.

2. Hver databehandler og, hvis det er relevant, databehandlerens repræsentant fører fortegnelser over alle kategorier af behandlingsaktiviteter, der foretages på vegne af en dataansvarlig, idet fortegnelsen skal indeholde:

a) navn på og kontaktoplysninger for databehandleren eller databehandlerne og for hver dataansvarlig, på hvis vegne databehandleren handler, samt, hvis det er relevant, den dataansvarliges eller databehandlerens repræsentant og databeskyttelsesrådgiveren

b) de kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige

c) hvor det er relevant, 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

d) hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1.

3. De fortegnelser, der er omhandlet i stk. 1 og 2, skal foreligge skriftligt, herunder elektronisk.

4. Den dataansvarlige eller databehandleren samt, hvis det er relevant, den dataansvarliges eller databehandlerens repræsentant stiller efter anmodning fortegnelserne til rådighed for tilsynsmyndigheden.

5. De i stk. 1 og 2 omhandlede forpligtelser finder ikke 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 lejlighedsvis, eller behandlingen omfatter særlige kategorier af oplysninger, jf. artikel 9, stk. 1, eller personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10.

Artikel 31

Samarbejde med tilsynsmyndigheden

Den dataansvarlige og databehandleren samt, hvis det er relevant, deres repræsentanter samarbejder efter anmodning med tilsynsmyndigheden i forbindelse med udførelsen af dens opgaver.

Afdeling 2

Personoplysningssikkerhed

Artikel 32

Behandlingssikkerhed

1. 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 foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

a) pseudonymisering og kryptering af personoplysninger

b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

3. 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 overholdelse af kravene i nærværende artikels stk. 1.

4. 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.

Artikel 33

Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden

1. 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 rettigheder eller frihedsrettigheder. Foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.

2. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden.

3. Den i stk. 1 omhandlede anmeldelse skal mindst:

a) 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 personoplysninger

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.

4. Når og for så vidt som det ikke er muligt at give oplysningerne samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.

5. Den dataansvarlige dokumenterer alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at denne artikel er overholdt.

Artikel 34

Underretning om brud på persondatasikkerheden til den registrerede

1. Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet på persondatasikkerheden.

2. Underretningen af den registrerede i henhold til denne artikels stk. 1 skal i et klart og forståeligt sprog 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).

3. Det er 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.

4. 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 stk. 3 er opfyldt.

Afdeling 3

Konsekvensanalyse vedrørende databeskyttelse og forudgående høring

Artikel 35

Konsekvensanalyse vedrørende databeskyttelse

1. 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.

2. Den dataansvarlige rådfører sig med databeskyttelsesrådgiveren, hvis en sådan er udpeget, når der foretages en konsekvensanalyse vedrørende databeskyttelse.

3. En konsekvensanalyse vedrørende databeskyttelse som omhandlet i stk. 1 er navnlig 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 oplysninger, 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.

4. Tilsynsmyndigheden udarbejder og offentliggør en liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse i henhold til stk. 1. Tilsynsmyndigheden indgiver disse lister til det i artikel 68 omhandlede Databeskyttelsesråd.

5. Tilsynsmyndigheden kan også udarbejde og offentliggøre en liste over de typer af behandlingsaktiviteter, for hvilke der ikke kræves nogen konsekvensanalyse vedrørende databeskyttelse. Tilsynsmyndigheden indgiver disse lister til Databeskyttelsesrådet.

6. Inden vedtagelsen af listerne i stk. 4 og 5 anvender den kompetente tilsynsmyndighed den sammenhængsmekanisme, der er omhandlet 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.

7. Analysen skal mindst 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.

8. 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.

9. Den dataansvarlige indhenter, hvis det er relevant, de registreredes eller deres repræsentanters synspunkter vedrørende den planlagte behandling, uden at det berører beskyttelse af kommercielle eller samfundsmæssige interesser eller behandlingsaktiviteternes sikkerhed.

10. Hvis behandling i henhold til artikel 6, stk. 1, litra c) eller e), 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 vedtagelsen af dette retsgrundlag, finder stk. 1-7 ikke anvendelse, medmindre medlemsstaterne anser det for nødvendigt at foretage en sådan analyse inden behandlingsaktiviteter.

11. Den dataansvarlige foretager, hvis det er nødvendigt, en fornyet gennemgang for at vurdere, hvorvidt behandling er foretaget i overensstemmelse med konsekvensanalysen vedrørende databeskyttelse, i hvert fald når der er en ændring af den risiko, som behandlingsaktiviteterne udgør.

Artikel 36

Forudgående høring

1. Den dataansvarlige hører tilsynsmyndigheden inden behandling, såfremt 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.

2. 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.

3. 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.

4. Medlemsstaterne hører 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.

5. 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.

Afdeling 4

Databeskyttelsesrådgiver

Artikel 37

Udpegelse af en databeskyttelsesrådgiver

1. Den dataansvarlige og databehandleren udpeger altid en databeskyttelsesrådgiver, når:

a) behandling foretages af en offentlig myndighed eller et offentligt organ, undtagen domstole, der handler i deres egenskab af domstol

b) den dataansvarliges eller databehandlerens kerneaktiviteter består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål kræver regelmæssig og systematisk overvågning af registrerede i stort omfang, eller

c) den 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.

2. En koncern kan udnævne en fælles databeskyttelsesrådgiver, forudsat at alle etableringer har let adgang til databeskyttelsesrådgiveren.

3. 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.

4. 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.

5. Databeskyttelsesrådgiveren udpeges på grundlag af sine faglige kvalifikationer, navnlig ekspertise inden for databeskyttelsesret og -praksis samt evne til at udføre de opgaver, der er omhandlet i artikel 39.

6. Databeskyttelsesrådgiveren kan være den dataansvarliges eller databehandlerens medarbejder eller kan udføre hvervet på grundlag af en tjenesteydelseskontrakt.

7. Den dataansvarlige eller databehandleren offentliggør kontaktoplysninger for databeskyttelsesrådgiveren og meddeler disse til tilsynsmyndigheden.

Artikel 38

Databeskyttelsesrådgiverens stilling

1. Den dataansvarlige og databehandleren sikrer, at databeskyttelsesrådgiveren inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger.

2. Den dataansvarlige og databehandleren støtter 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.

3. Den dataansvarlige og databehandleren sikrer, at databeskyttelsesrådgiveren ikke modtager instrukser vedrørende udførelsen af disse opgaver. Den pågældende må ikke afskediges eller straffes af den dataansvarlige eller databehandleren for at udføre sine opgaver. Databeskyttelsesrådgiveren rapporterer direkte til det øverste ledelsesniveau hos den dataansvarlige eller databehandleren.

4. Registrerede kan kontakte databeskyttelsesrådgiveren angående alle spørgsmål om behandling af deres oplysninger og om udøvelse af deres rettigheder i henhold til denne forordning.

5. Databeskyttelsesrådgiveren er underlagt tavshedspligt eller fortrolighed vedrørende udførelsen af sine opgaver i overensstemmelse med EU-retten eller medlemsstaternes nationale ret.

6. Databeskyttelsesrådgiveren kan udføre andre opgaver og have andre pligter. Den dataansvarlige eller databehandleren sikrer, at sådanne opgaver og pligter ikke medfører en interessekonflikt.

Artikel 39

Databeskyttelsesrådgiverens opgaver

1. Databeskyttelsesrådgiveren har som minimum følgende opgaver:

a) at underrette og rådgive den dataansvarlige eller databehandleren og de ansatte, der behandler personoplysninger, om deres forpligtelser i henhold til denne forordning og anden EU-ret eller national ret i medlemsstaterne om databeskyttelse

b) at overvåge overholdelsen af denne forordning, 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 det 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.

2. Databeskyttelsesrådgiveren tager under udførelsen af sine opgaver behørigt hensyn til den risiko, der er forbundet med behandlingsaktiviteter, under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål.

Afdeling 5

Adfærdskodekser og certificering

Artikel 40

Adfærdskodekser

1. Medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen tilskynder 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 denne forordning.

2. 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.

3. Adfærdskodekser, der er godkendt i henhold til denne artikels stk. 5 og er generelt gyldige i henhold til denne artikels stk. 9, kan — ud over overholdelse af de dataansvarlige eller databehandlere, der er omfattet af denne forordning — også overholdes af dataansvarlige eller databehandlere, der i henhold til artikel 3 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). Sådanne dataansvarlige eller databehandlere skal, gennem kontrakter eller andre retligt bindende instrumenter, afgive bindende tilsagn, som kan håndhæves, om at anvende disse fornødne garantier, herunder for så vidt angår registreredes rettigheder.

4. En adfærdskodeks omhandlet i denne artikels 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.

5. Sammenslutninger og andre organer omhandlet i denne artikels stk. 2, der har til hensigt at udarbejde en adfærdskodeks eller at ændre eller udvide en eksisterende adfærdskodeks, forelægger et udkast til kodeks, ændring eller udvidelse for den tilsynsmyndighed, der er kompetent i henhold til artikel 55. 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.

6. 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, registrerer og offentliggør tilsynsmyndigheden kodeksen.

7. Hvis et udkast til adfærdskodeks vedrører behandlingsaktiviteter i flere medlemsstater, forelægger den tilsynsmyndighed, der er kompetent i henhold til artikel 55, inden godkendelsen af udkastet til kodeks, ændring eller udvidelse, efter proceduren i artikel 63 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 denne artikels stk. 3.

8. 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.

9. Kommissionen kan ved hjælp af gennemførelsesretsakter afgøre, at den godkendte adfærdskodeks, ændring eller udvidelse, som den har modtaget i henhold til denne artikels stk. 8, generelt er gyldige i Unionen. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

10. Kommissionen tilser, at de godkendte kodekser, som i henhold til Kommissionen har generel gyldighed, jf. stk. 9, offentliggøres på passende vis.

11. Databeskyttelsesrådet samler alle godkendte adfærdskodekser, ændringer og udvidelser i et register og gør dem offentligt tilgængelige på passende vis.

Artikel 41

Kontrol af godkendte adfærdskodekser

1. Uden at dette berører den kompetente tilsynsmyndigheds opgaver og beføjelser i henhold til artikel 57 og 58, kan kontrol af overholdelsen af en adfærdskodeks i henhold til artikel 40 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.

2. 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.

3. Den kompetente tilsynsmyndighed forelægger 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.

4. Uden at dette berører den kompetente tilsynsmyndigheds opgaver og beføjelser eller bestemmelserne i kapitel VIII, træffer et organ som omhandlet i denne artikels stk. 1 under forudsætning af fornødne garantier de nødvendige foranstaltninger i tilfælde af en dataansvarligs eller databehandlers overtrædelse af kodeksen, herunder suspension eller udelukkelse af den dataansvarlige eller databehandleren fra kodeksen. Organet underretter den kompetente tilsynsmyndighed om sådanne foranstaltninger og begrundelsen for at have truffet dem.

5. 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.

6. Denne artikel finder ikke anvendelse på behandling, der udføres af offentlige myndigheder og organer.

Artikel 42

Certificering

1. Medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen tilskynder 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 denne forordning. Mikrovirksomheders og små og mellemstore virksomheders særlige behov tages i betragtning.

2. Certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger eller -mærker, der er godkendt i henhold til denne artikels stk. 5, kan — ud over overholdelse af de dataansvarlige eller databehandlere, der er omfattet af denne forordning — 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). Disse dataansvarlige eller databehandlere skal, gennem kontrakter eller andre retligt bindende instrumenter, afgive bindende tilsagn, som kan håndhæves, om at anvende disse fornødne garantier, herunder for så vidt angår registreredes rettigheder.

3. Certificering skal være frivillig og tilgængelig gennem en gennemsigtig proces.

4. Certificering i henhold til denne artikel indskrænker ikke den dataansvarliges eller databehandlerens ansvar for at overholde denne forordning og berører ikke opgaverne og beføjelserne for de tilsynsmyndigheder, der er kompetente i henhold til artikel 55 eller 56.

5. Certificering i henhold til denne artikel 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. Hvis kriterierne er godkendt af Databeskyttelsesrådet, kan det føre til en fælles certificering, Den Europæiske Databeskyttelsesmærkning.

6. Den dataansvarlige eller databehandler, der forelægger sin behandling for certificeringsmekanismen, giver 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.

7. 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. 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.

8. Databeskyttelsesrådet samler alle certificeringsmekanismer og databeskyttelsesmærkninger og -mærker i et register og gør dem offentligt tilgængelige på passende vis.

Artikel 43

Certificeringsorganer

1. Uden at dette berører den kompetente tilsynsmyndigheds opgaver og beføjelser i henhold til artikel 57 og 58, udsteder og forlænger certificeringsorganer, der har et passende ekspertiseniveau for så vidt angår databeskyttelse, 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. 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 ([1]) 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.

2. Certificeringsorganer som omhandlet i stk. 1 akkrediteres kun i overensstemmelse med nævnte stykke, hvis de har:

a) påvist deres uafhængighed og ekspertise med hensyn til certificeringens genstand til den kompetente tilsynsmyndigheds tilfredshed

([1]) 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).

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.

3. Akkreditering af de i denne artikels 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. I tilfælde af akkreditering i henhold til nærværende artikels stk. 1, litra b), supplerer disse krav kravene i forordning (EF) nr. 765/2008 og de tekniske regler, der beskriver certificeringsorganers metoder og procedurer.

4. 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. Akkreditering udstedes for en periode på højst fem år og kan forlænges på samme betingelser, såfremt certificeringsorganet opfylder de i denne artikel fastsatte krav.

5. De i stk. 1 omhandlede certificeringsorganer giver de kompetente tilsynsmyndigheder oplysninger om begrundelsen for at udstede eller tilbagetrække den certificering, der er anmodet om.

6. Tilsynsmyndigheden offentliggør de i denne artikels stk. 3 omhandlede krav og de i artikel 42, stk. 5, omhandlede kriterier i lettilgængelig form. Tilsynsmyndighederne meddeler også disse krav og kriterier til Databeskyttelsesrådet. Databeskyttelsesrådet samler alle certificeringsmekanismer og databeskyttelsesmærkninger i et register og gør dem offentligt tilgængelige på passende vis.

7. Uden at dette berører kapitel VIII, tilbagekalder den kompetente tilsynsmyndighed eller det nationale akkrediteringsorgan en akkreditering af et certificeringsorgan, jf. denne artikels stk. 1, hvis betingelserne for akkrediteringen ikke er eller ikke længere er opfyldt, eller hvis de foranstaltninger, som organet har truffet, overtræder denne forordning.

8. 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.

9. 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. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

KAPITEL V

Overførsler af personoplysninger til tredjelande eller internationale organisationer

Artikel 44

Generelt princip for overførsler

Enhver overførsel af personoplysninger, som underkastes behandling eller planlægges behandlet efter overførsel til et tredjeland eller en international organisation, må kun finde sted, hvis betingelserne i dette kapitel med forbehold af de øvrige bestemmelser i denne forordning opfyldes af den dataansvarlige og databehandleren, herunder ved videreoverførsel af personoplysninger fra det pågældende tredjeland eller den pågældende internationale organisation til et andet tredjeland eller en anden international organisation. Alle bestemmelserne i dette kapitel anvendes for at sikre, at det beskyttelsesniveau, som fysiske personer garanteres i medfør af denne forordning, ikke undermineres.

Artikel 45

Overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet

1. Overførsel af personoplysninger til et tredjeland eller en international organisation kan finde sted, hvis Kommissionen har fastslået, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation har et tilstrækkeligt beskyttelsesniveau. En sådan overførsel kræver ikke specifik godkendelse.

2. Ved vurdering af beskyttelsesniveauets tilstrækkelighed tager Kommissionen navnlig følgende elementer i betragtning:

a) retsstatsprincippet, respekt for menneskerettighederne og de grundlæggende frihedsrettigheder, relevant lovgivning, både generel og sektorbestemt, herunder vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og strafferet og offentlige myndigheders adgang til personoplysninger, samt gennemførelsen af sådan lovgivning, databeskyttelsesregler, faglige regler og sikkerhedsforanstaltninger, herunder regler for videreoverførsel af personoplysninger til et andet tredjeland eller en anden international organisation, der gælder i dette land eller denne internationale organisation, retspraksis samt effektive rettigheder for registrerede, som kan håndhæves, og effektiv administrativ og retslig prøvelse for de registrerede, hvis personoplysninger overføres

b) tilstedeværelse af en eller flere velfungerende uafhængige tilsynsmyndigheder i tredjelandet, eller som den internationale organisation er underlagt, med ansvar for at sikre og håndhæve, at databeskyttelsesreglerne overholdes, herunder tilstrækkelige håndhævelsesbeføjelser, for at bistå og rådgive de registrerede, når de udøver deres rettigheder, og for samarbejde med tilsynsmyndighederne i medlemsstaterne, og

c) de internationale forpligtelser, som tredjelandet eller den internationale organisation har påtaget sig, eller andre forpligtelser, der følger af retligt bindende konventioner eller instrumenter og af landets eller organisationens deltagelse i multilaterale eller regionale systemer, navnlig vedrørende beskyttelse af personoplysninger.

3. Kommissionen kan efter vurdering af beskyttelsesniveauets tilstrækkelighed ved hjælp af en gennemførelsesretsakt fastslå, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland, eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2. I den pågældende gennemførelsesretsakt fastsættes en mekanisme for regelmæssig revision, som foretages mindst hvert fjerde år, og som inddrager enhver relevant udvikling i tredjelandet eller den internationale organisation. I gennemførelsesretsakten angives dennes territoriale og sektorbestemte anvendelsesområde og i påkommende tilfælde den eller de tilsynsmyndigheder, der er omhandlet i denne artikels stk. 2, litra b). Gennemførelsesretsakten vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

4. Kommissionen overvåger løbende udvikling i tredjelande og internationale organisationer, der kan påvirke virkningen af afgørelser, der er vedtaget i henhold til denne artikels stk. 3, og afgørelser og beslutninger, der er vedtaget på grundlag af artikel 25, stk. 6, i direktiv 95/46/EF.

5. Kommissionen ophæver, ændrer eller suspenderer i det omfang, det er nødvendigt, uden tilbagevirkende kraft afgørelsen omhandlet i denne artikels stk. 3 ved hjælp af gennemførelsesretsakter, hvis tilgængelige oplysninger, navnlig efter den i denne artikels stk. 3 omhandlede revision, viser, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland, eller en international organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

I behørigt begrundede særligt hastende tilfælde vedtager Kommissionen efter proceduren i artikel 93, stk. 3, gennemførelsesretsakter, der finder anvendelse straks.

6. Kommissionen fører konsultationer med tredjelandet eller den internationale organisation med henblik på at afhjælpe den situation, der har givet anledning til en afgørelse vedtaget i henhold til stk. 5.

7. En afgørelse som angivet i denne artikels stk. 5 berører ikke overførsel af personoplysninger til det pågældende tredjeland, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation i medfør af artikel 46-49.

8. Kommissionen offentliggør i *Den Europæiske Unions Tidende* og på sit websted en liste over tredjelande, områder og specifikke sektorer i tredjelande samt internationale organisationer, som den har fastslået sikrer eller ikke længere sikrer et tilstrækkeligt beskyttelsesniveau.

9. Afgørelser og beslutninger, der er vedtaget af Kommissionen på grundlag af artikel 25, stk. 6, i direktiv 95/46/EF, gælder fortsat, indtil de ændres, erstattes eller ophæves ved en kommissionsafgørelse, der vedtages i henhold til nærværende artikels stk. 3 eller 5.

Artikel 46

Overførsler omfattet af fornødne garantier

1. Hvis der ikke er vedtaget en afgørelse i henhold til artikel 45, stk. 3, må en dataansvarlig eller databehandler kun overføre personoplysninger til et tredjeland eller en international organisation, hvis vedkommende har givet de fornødne garantier, og på betingelse af at rettigheder, som kan håndhæves, og effektive retsmidler for registrerede er tilgængelige.

2. De fornødne garantier i stk. 1 kan uden krav om specifik godkendelse fra en tilsynsmyndighed sikres gennem:

a) et retligt bindende instrument, som kan håndhæves, mellem offentlige myndigheder eller organer

b) bindende virksomhedsregler i overensstemmelse med artikel 47

c) standardbestemmelser om databeskyttelse vedtaget af Kommissionen efter undersøgelsesproceduren i artikel 93, stk. 2

d) standardbestemmelser om databeskyttelse vedtaget af en tilsynsmyndighed og godkendt af Kommissionen efter undersøgelsesproceduren i artikel 93, stk. 2

e) 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, eller

f) 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.

3. Med forbehold af godkendelse fra den kompetente tilsynsmyndighed kan de fornødne garantier i stk. 1 også sikres gennem navnlig:

a) kontraktbestemmelser mellem den dataansvarlige eller databehandleren og den dataansvarlige, databehandleren eller modtageren af personoplysninger i tredjelandet eller den internationale organisation, eller

b) bestemmelser, der medtages i administrative ordninger mellem offentlige myndigheder eller organer, og som omfatter effektive rettigheder, som kan håndhæves, for registrerede.

4. Tilsynsmyndigheden anvender den sammenhængsmekanisme, der er omhandlet i artikel 63, i de tilfælde, der er omhandlet i nærværende artikels stk. 3.

5. Godkendelser fra en medlemsstat eller en tilsynsmyndighed på grundlag af artikel 26, stk. 2, i direktiv 95/46/EF er gyldige, indtil de om nødvendigt ændres, erstattes eller ophæves af den pågældende tilsynsmyndighed. Afgørelser og beslutninger, der er vedtaget af Kommissionen på grundlag af artikel 26, stk. 4, i direktiv 95/46/EF, er i kraft, indtil de om nødvendigt ændres, erstattes eller ophæves ved en kommissionsafgørelse, der vedtages i henhold til nærværende artikels stk. 2.

Artikel 47

Bindende virksomhedsregler

1. I overensstemmelse med den sammenhængsmekanisme, der er omhandlet i artikel 63, godkender den kompetente tilsynsmyndighed bindende virksomhedsregler, såfremt de:

a) er retligt bindende og gælder for og håndhæves af alle berørte medlemmer i den koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet, herunder deres medarbejdere

b) udtrykkeligt tillægger registrerede rettigheder, som kan håndhæves, for så vidt angår behandling af deres personoplysninger, og

c) opfylder kravene i stk. 2.

2. De bindende virksomhedsregler i stk. 1 skal mindst angive:

a) strukturen i og kontaktoplysningerne for den koncern eller gruppe af foretagender, der er udøver en fælles økonomisk aktivitet, og hvert af dens medlemmer

b) overførslerne eller rækken af overførsler af oplysninger, herunder kategorier af personoplysninger, behandlingstype og -formål, typen af berørte registrerede og angivelse af det pågældende tredjeland eller de pågældende tredjelande

c) deres retligt bindende karakter, både internt og eksternt

d) anvendelsen af de generelle databeskyttelsesprincipper, navnlig formålsbegrænsning, dataminimering, begrænsede opbevaringsperioder, datakvalitet, databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, retsgrundlag for behandling, behandling af særlige kategorier af personoplysninger, foranstaltninger til at sikre datasikkerhed og krav til videreoverførsel til organer, der ikke er underlagt de bindende virksomhedsregler

e) de registreredes rettigheder med hensyn til behandling og midler til at udøve disse rettigheder, herunder til ikke at blive gjort til genstand for afgørelser, som alene er truffet på grundlag af automatisk behandling, herunder profilering, jf. artikel 22, samt retten til at indgive klage til den kompetente tilsynsmyndighed og de kompetente domstole i medlemsstaterne, jf. artikel 79, og til at modtage godtgørelse og, hvis det er relevant, erstatning for brud på de bindende virksomhedsregler

f) den dataansvarliges eller databehandlerens accept af ansvaret for ethvert brud på de bindende virksomhedsregler, der begås af en berørt virksomhed i koncernen, som ikke er etableret i Unionen, når den dataansvarlige eller databehandleren er etableret inden for en medlemsstats område; den dataansvarlige eller databehandleren fritages kun helt eller delvis for dette ansvar, hvis vedkommende beviser, at den pågældende virksomhed ikke er skyld i den begivenhed, der medførte skaden

g) hvordan informationen om bindende virksomhedsregler, navnlig de bestemmelser, der er omhandlet i litra d), e) og f), gives til de registrerede ud over den information, der er omhandlet i artikel 13 og 14

h) opgaverne for enhver databeskyttelsesrådgiver, der er udpeget i henhold til artikel 37, eller enhver anden person eller enhed med ansvar for overvågning af overholdelse af de bindende virksomhedsregler inden for koncernen eller gruppen af foretagender, der udøver en fælles økonomisk aktivitet, samt overvågning af uddannelse og håndtering af klager

i) klageprocedurerne

j) de mekanismer i koncernen eller gruppen af foretagender, der udøver en fælles økonomisk aktivitet, som skal sikre kontrol af overholdelse af de bindende virksomhedsregler. Sådanne mekanismer skal omfatte databeskyttelsesrevisioner og metoder til at sikre korrigerende foranstaltninger med henblik på at beskytte de registreredes rettigheder. Resultaterne af denne revision bør meddeles den person eller enhed, der er omhandlet i litra h), og bestyrelsen i kontrolvirksomheden i en koncern eller i gruppen af foretagender, der udøver en fælles økonomisk aktivitet, og bør være tilgængelige på anmodning af den kompetente tilsynsmyndighed

k) mekanismerne til indberetning og registrering af ændringer af reglerne og indberetning af disse ændringer til tilsynsmyndigheden

l) den mekanisme til samarbejde med tilsynsmyndigheden, som har til formål at sikre, at alle virksomheder i koncernen eller gruppen af foretagender, der udøver en fælles økonomisk aktivitet, overholder reglerne, navnlig ved at forelægge tilsynsmyndigheden resultaterne af revisionen af de foranstaltninger, der er omhandlet i litra j)

m) mekanismerne til indberetning til den kompetente tilsynsmyndighed af retlige forpligtelser, som en virksomhed i koncernen eller gruppen af foretagender, der udøver en fælles økonomisk aktivitet, er omfattet af i et tredjeland, og som sandsynligvis vil have betydelig negativ indvirkning på garantierne i de bindende virksomhedsregler, og

n) den passende databeskyttelsesuddannelse, som personale, der har permanent eller regelmæssig adgang til personoplysninger, skal følge.

3. Kommissionen kan angive formatet og procedurerne for udveksling af oplysninger mellem dataansvarlige, databehandlere og tilsynsmyndigheder for bindende virksomhedsregler som omhandlet i denne artikel. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

Artikel 48

Overførsel eller videregivelse uden hjemmel i EU-retten

Enhver dom afsagt af en domstol eller ret og enhver afgørelse truffet af en administrativ myndighed i et tredjeland, der kræver, at en dataansvarlig eller en databehandler overfører eller videregiver personoplysninger, kan kun anerkendes eller håndhæves på nogen måde, hvis den bygger på en international aftale, såsom en traktat om gensidig retshjælp mellem det anmodende tredjeland og Unionen eller en medlemsstat, uden at det berører andre grunde til overførsel i henhold til dette kapitel.

Artikel 49

Undtagelser i særlige situationer

1. I mangel af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 45, stk. 3, eller fornødne garantier i henhold til artikel 46, herunder bindende virksomhedsregler, må en overførsel eller flere overførsler af personoplysninger til et tredjeland eller en international organisation kun finde sted på en af følgende betingelser:

a) den registrerede udtrykkelig har givet samtykke til den foreslåede overførsel efter at være blevet informeret om de mulige risici, som sådanne overførsler kan medføre for den registrerede på grund af den manglende afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller fornødne garantier

b) overførslen er nødvendig af hensyn til opfyldelse af en kontrakt mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en sådan kontrakt

c) overførslen er nødvendig af hensyn til indgåelse eller opfyldelse af en kontrakt, der i den registreredes interesse indgås mellem den dataansvarlige og en anden fysisk eller juridisk person

d) overførslen er nødvendig af hensyn til vigtige samfundsinteresser

e) overførslen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares

f) overførslen er nødvendig for at beskytte den registreredes eller andre personers vitale interesser, hvis den registrerede ikke fysisk eller juridisk er i stand til at give samtykke

g) overførslen finder sted fra et register, der ifølge EU-ret eller medlemsstaternes nationale ret er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri, men kun i det omfang de ved EU-ret eller medlemsstaternes nationale ret fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde

Hvis overførsel ikke kan have hjemmel i en bestemmelse i artikel 45 eller 46, herunder bestemmelserne om bindende virksomhedsregler, og ingen af undtagelserne i særlige situationer omhandlet i dette stykkes første afsnit finder anvendelse, må en videregivelse til et tredjeland eller en international organisation kun finde sted, hvis overførslen ikke gentages, kun vedrører et begrænset antal registrerede, er nødvendig af hensyn til vægtige legitime interesser, som forfølges af den dataansvarlige, den registreredes interesser eller rettigheder og frihedsrettigheder ikke går forud for disse interesser, og den dataansvarlige har vurderet alle omstændigheder i forbindelse med overførslen og på grundlag af denne vurdering giver passende garantier for beskyttelse af personoplysningerne. Den dataansvarlige underretter tilsynsmyndigheden om overførslen. Ud over oplysningerne i artikel 13 og 14 underretter den dataansvarlige den registrerede om overførslen og om de vægtige legitime interesser, der forfølges.

2. En overførsel i henhold til stk. 1, første afsnit, litra g), må ikke omfatte alle personoplysninger eller hele kategorier af personoplysninger i et register. Når et register er beregnet til at blive konsulteret af personer, der har en legitim interesse heri, må overførsel kun ske på anmodning af disse personer, eller hvis de skal være modtagerne.

3. Stk. 1, første afsnit, litra a), b) og c), og stk. 1, andet afsnit, finder ikke anvendelse på aktiviteter, der gennemføres af offentlige myndigheder som led udøvelsen af deres offentligretlige beføjelser.

4. De samfundsinteresser, der er omhandlet i stk. 1, første afsnit, litra d), skal være anerkendt i EU-retten eller retten i den medlemsstat, som den dataansvarlige er underlagt.

5. Hvis der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, kan EU-retten eller medlemsstaternes nationale ret af hensyn til vigtige samfundsinteresser udtrykkelig fastsætte grænser for overførsel af særlige kategorier af oplysninger til et tredjeland eller en international organisation. Medlemsstaterne giver Kommissionen meddelelse om disse bestemmelser.

6. Den dataansvarlige eller databehandleren dokumenterer vurderingen og de passende garantier i denne artikels stk. 1, andet afsnit, i de fortegnelser, der er omhandlet i artikel 30.

Artikel 50

Internationalt samarbejde om beskyttelse af personoplysninger

Kommissionen og tilsynsmyndighederne træffer i forhold til tredjelande og internationale organisationer de nødvendige foranstaltninger til at:

a) udvikle internationale samarbejdsmekanismer med henblik på at lette effektiv håndhævelse af lovgivningen om beskyttelse af personoplysninger

b) yde international gensidig bistand i håndhævelse af lovgivningen om beskyttelse af personoplysninger, herunder gennem anmeldelse, indbringelse af klager, efterforskningsbistand og informationsudveksling, under iagttagelse af de fornødne garantier for beskyttelse af personoplysninger og andre grundlæggende rettigheder og frihedsrettigheder

c) inddrage relevante interessenter i drøftelser og aktiviteter, der har til formål at fremme det internationale samarbejde om håndhævelse af lovgivningen om beskyttelse af personoplysninger

d) fremme udveksling og dokumentation af lovgivning om beskyttelse af personoplysninger og praksis på området, herunder om kompetencekonflikter med tredjelande.

KAPITEL VI

Uafhængige tilsynsmyndigheder

Afdeling 1

Uafhængig status

Artikel 51

Tilsynsmyndighed

1. Hver medlemsstat sikrer, at en eller flere uafhængige offentlige myndigheder er ansvarlige for at føre tilsyn med anvendelsen af denne forordning, for at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling og for at lette fri udveksling af personoplysninger i Unionen (»tilsynsmyndighed«).

2. Hver enkelt tilsynsmyndighed bidrager til ensartet anvendelse af denne forordning i hele Unionen. Til dette formål samarbejder tilsynsmyndighederne med hinanden og med Kommissionen i henhold til kapitel VII.

3. Hvis der er mere end én tilsynsmyndighed i en medlemsstat, udpeger den pågældende medlemsstat en tilsynsmyndighed, der skal repræsentere disse myndigheder i Databeskyttelsesrådet, og fastsætter en mekanisme, som sikrer, at de andre myndigheder overholder reglerne vedrørende den sammenhængsmekanisme, der er omhandlet i artikel 63.

4. Hver medlemsstat giver senest den 25. maj 2018 Kommissionen meddelelse om de bestemmelser, som den vedtager i henhold til dette kapitel, og underretter den straks om alle senere ændringer, der berører dem.

Artikel 52

Uafhængighed

1. Hver tilsynsmyndighed udfører sine opgaver og udøver sine beføjelser i henhold til denne forordning i fuld uafhængighed.

2. Medlemmet eller medlemmerne af hver tilsynsmyndighed skal i forbindelse med udførelsen af deres opgaver og udøvelsen af deres beføjelser i henhold til denne forordning være frie for udefrakommende indflydelse, det være sig direkte eller indirekte, og må hverken søge eller modtage instrukser fra andre.

3. Et medlem eller medlemmer af den enkelte tilsynsmyndighed skal afholde sig fra enhver handling, der er uforenelig med deres hverv, og må ikke, så længe deres embedsperiode varer, udøve uforenelig lønnet eller ulønnet virksomhed.

4. Hver medlemsstat sikrer, at den enkelte tilsynsmyndighed råder over de nødvendige menneskelige, tekniske og finansielle ressourcer samt lokaler og infrastruktur til effektivt at kunne udføre sine opgaver og udøve sine beføjelser, herunder opgaver og beføjelser vedrørende gensidig bistand samt samarbejde med og deltagelse i Databeskyttelsesrådet.

5. Hver medlemsstat sikrer, at den enkelte tilsynsmyndighed vælger og råder over sit eget personale, der alene er under ledelse af medlemmet eller medlemmerne af den pågældende tilsynsmyndighed.

6. Hver medlemsstat sikrer, at den enkelte tilsynsmyndighed er underlagt finansiel kontrol, som ikke påvirker dens uafhængighed, og at den fører særskilte, offentlige årsbudgetter, der kan være en del af det samlede statsbudget eller nationale budget.

Artikel 53

Generelle betingelser for medlemmer af en tilsynsmyndighed

1. Medlemsstaterne sikrer, at hvert medlem af en tilsynsmyndighed udnævnes efter en gennemsigtig procedure af:

— deres parlament

— deres regering

— deres statschef, eller

— et uafhængigt organ, der i henhold til medlemsstaternes nationale ret har fået overdraget ansvaret for udnævnelsen.

2. Hvert medlem skal have de kvalifikationer, den erfaring og den kompetence, navnlig på området beskyttelse af personoplysninger, der er nødvendige for at varetage dets hverv og udøve dets beføjelser.

3. Et medlems hverv ophører ved udløbet af embedsperioden, ved frivillig fratrædelse eller ved obligatorisk fratrædelse i overensstemmelse med den pågældende medlemsstats nationale ret.

4. Et medlem må kun afskediges i tilfælde af alvorligt embedsmisbrug, eller hvis medlemmet ikke længere opfylder betingelserne for at varetage sit hverv.

Artikel 54

Regler om oprettelse af en tilsynsmyndighed

1. Hver medlemsstat fastsætter ved lov alle af følgende:

a) den enkelte tilsynsmyndigheds oprettelse

b) de nødvendige kvalifikationer og udvælgelseskriterier, der skal være opfyldt for at kunne blive udnævnt til medlem af den enkelte tilsynsmyndighed

c) reglerne og procedurerne for udnævnelse af medlemmet eller medlemmerne af den enkelte tilsynsmyndighed

d) embedsperioden for medlemmet eller medlemmerne af den enkelte tilsynsmyndighed på mindst fire år, med undtagelse af den første udnævnelse efter den 24. maj 2016, som kan være af kortere varighed, hvis det er nødvendigt for at beskytte den pågældende tilsynsmyndigheds uafhængighed ved hjælp af en forskudt udnævnelsesprocedure

e) om og i bekræftende fald for hvor mange embedsperioder medlemmet eller medlemmerne af den enkelte tilsynsmyndighed kan genudnævnes

f) betingelserne vedrørende forpligtelser for den enkelte tilsynsmyndigheds medlem eller medlemmer og personale, forbud mod handlinger, hverv og fordele, der er uforenelige hermed, under og efter embedsperioden, og regler for arbejdsophør.

2. Den enkelte tilsynsmyndigheds medlem eller medlemmer og personale har i overensstemmelse med EU-retten eller medlemsstaternes nationale ret såvel under som efter deres embedsperiode tavshedspligt for så vidt angår alle fortrolige oplysninger, der er kommet til deres kendskab under udførelsen af deres opgaver eller udøvelsen af deres beføjelser. I deres embedsperiode gælder denne tavshedspligt især indberetninger fra fysiske personer af overtrædelser af denne forordning.

Afdeling 2

Kompetence, opgaver og beføjelser

Artikel 55

Kompetence

1. Hver tilsynsmyndighed er kompetent til at udføre de opgaver og udøve de beføjelser, der tillægges den i overensstemmelse med denne forordning, på sin egen medlemsstats område.

2. Hvis behandling foretages af offentlige myndigheder eller af private organer, der handler på grundlag af artikel 6, stk. 1, litra c) eller e), er tilsynsmyndigheden i den pågældende medlemsstat kompetent. I så fald finder artikel 56 ikke anvendelse.

3. Tilsynsmyndigheder er ikke kompetente til at føre tilsyn med domstoles behandlingsaktiviteter, når disse handler i deres egenskab af domstol.

Artikel 56

Den ledende tilsynsmyndigheds kompetence

1. 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.

2. Uanset stk. 1 er hver tilsynsmyndighed kompetent til at behandle en indgivet klage eller en eventuel overtrædelse af denne forordning, hvis genstanden alene vedrører en etablering i dens medlemsstat eller alene i væsentlig grad påvirker registrerede i dens medlemsstat.

3. I de i denne artikels stk. 2 omhandlede tilfælde underretter tilsynsmyndigheden straks den ledende tilsynsmyndighed om dette forhold. Den ledende tilsynsmyndighed beslutter inden for en frist på tre uger efter at være blevet underrettet, om den vil behandle sagen efter proceduren i artikel 60 under hensyntagen til, hvorvidt den dataansvarlige eller databehandleren er etableret i den underrettende tilsynsmyndigheds medlemsstat

4. Hvis den ledende tilsynsmyndighed beslutter at behandle sagen, finder proceduren i artikel 60 anvendelse. Den tilsynsmyndighed, der underrettede den ledende tilsynsmyndighed, kan forelægge den ledende tilsynsmyndighed et udkast til afgørelse. Den ledende tilsynsmyndighed tager størst muligt hensyn til dette udkast, når den udarbejder udkastet til afgørelse, jf. artikel 60, stk. 3.

5. Beslutter den ledende tilsynsmyndighed ikke at behandle sagen, behandler den tilsynsmyndighed, der forelagde sagen for den ledende tilsynsmyndighed, sagen i overensstemmelse med artikel 61 og 62.

6. Den ledende tilsynsmyndighed er den dataansvarliges eller databehandlerens eneste kontakt i forbindelse med den grænseoverskridende behandling, der foretages af denne dataansvarlige eller databehandler.

Artikel 57

Opgaver

1. Uden at dette berører andre opgaver, der er fastsat i denne forordning, skal hver tilsynsmyndighed på sit område:

a) føre tilsyn med og håndhæve anvendelsen af denne forordning

b) fremme offentlighedens kendskab til og forståelse af risici, regler, garantier og rettigheder i forbindelse med behandling Der skal sættes særlig fokus på aktiviteter, der er direkte rettet mod børn

c) i henhold til medlemsstaternes nationale ret rådgive det nationale parlament, regeringen og andre institutioner og organer om lovgivningsmæssige og administrative foranstaltninger til beskyttelse af fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling

d) fremme dataansvarliges og databehandleres kendskab til deres forpligtelser i henhold til denne forordning

e) efter anmodning informere registrerede om udøvelse af deres rettigheder i henhold til denne forordning og med henblik herpå samarbejde med tilsynsmyndighederne i andre medlemsstater, hvis det er relevant

f) behandle klager, der indgives af en registreret eller af et organ, en organisation eller en sammenslutning i overensstemmelse med artikel 80, og, for så vidt det er hensigtsmæssigt, undersøge genstanden for klagen og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist, navnlig hvis yderligere undersøgelse eller koordinering med en anden tilsynsmyndighed er nødvendig

g) samarbejde med andre tilsynsmyndigheder, herunder gennem udveksling af oplysninger og gensidig bistand, med henblik på at sikre ensartet anvendelse og håndhævelse af denne forordning

h) gennemføre undersøgelser om anvendelsen af denne forordning, herunder på grundlag af oplysninger, der er modtaget fra en anden tilsynsmyndighed eller en anden offentlig myndighed

i) holde øje med relevant udvikling, for så vidt den har indvirkning på beskyttelse af personoplysninger, navnlig udviklingen inden for informations- og kommunikationsteknologi og handelspraksis

j) vedtage standardkontraktbestemmelser som omhandlet i artikel 28, stk. 8, og i artikel 46, stk. 2, litra d)

k) opstille og føre en liste i forbindelse med kravet om en konsekvensanalyse vedrørende databeskyttelse i henhold til artikel 35, stk. 4

l) rådgive om behandlingsaktiviteter som omhandlet i artikel 36, stk. 2

m) tilskynde til udarbejdelse af adfærdskodekser i henhold til artikel 40, stk. 1, og afgive udtalelse om og godkende sådanne adfærdskodekser, som sikrer tilstrækkelige garantier i henhold til artikel 40, stk. 5

n) tilskynde til fastlæggelse af certificeringsmekanismer for databeskyttelse og databeskyttelsesmærkninger og -mærker i henhold til artikel 42, stk. 1, og godkende kriterierne for certificering i henhold til artikel 42, stk. 5

o) når det er relevant, regelmæssigt gennemgå certificeringer udstedt i henhold til artikel 42, stk. 7

p) opstille og offentliggøre kriterierne for akkreditering af et organ til kontrol af adfærdskodekser i henhold til artikel 41 og af et certificeringsorgan i henhold til artikel 43

q) foretage akkreditering af et organ til kontrol af adfærdskodekser i henhold til artikel 41 og af et certificeringsorgan i henhold til artikel 43

r) godkende kontraktbestemmelser og bestemmelser som omhandlet i artikel 46, stk. 3

s) godkende bindende virksomhedsregler i henhold til artikel 47

t) bidrage til Databeskyttelsesrådets aktiviteter

u) føre interne fortegnelser over overtrædelser af denne forordning og over foranstaltninger, der er truffet i henhold til artikel 58, stk. 2, og

v) udføre enhver anden opgave i forbindelse med beskyttelse af personoplysninger.

2. Hver tilsynsmyndighed letter indgivelse af klager, jf. stk. 1, litra f), gennem foranstaltninger som f.eks. en klageformular, der også kan udfyldes elektronisk, uden at udelukke andre kommunikationsmidler.

3. Hver tilsynsmyndighed varetager sine opgaver uden udgifter for den registrerede og, hvis det er relevant, for databeskyttelsesrådgiveren.

4. Hvis anmodninger er åbenbart grundløse eller uforholdsmæssige, især fordi de gentages, kan tilsynsmyndigheden opkræve et rimeligt gebyr baseret på de administrative omkostninger eller afvise at efterkomme anmodningen. Bevisbyrden for, at anmodningen er åbenbart grundløs eller uforholdsmæssig, påhviler tilsynsmyndigheden.

Artikel 58

Beføjelser

1. Hver tilsynsmyndighed har alle af følgende undersøgelsesbeføjelser:

a) at give den dataansvarlige og databehandleren samt den dataansvarliges eller databehandlerens eventuelle repræsentant påbud om at give alle oplysninger, der kræves til udførelse af myndighedens opgaver

b) at foretage undersøgelser i form af databeskyttelsesrevisioner

c) at foretage en revision af certificeringer udstedt i henhold til artikel 42, stk. 7

d) at underrette den dataansvarlige eller databehandleren om en påstået overtrædelse af denne forordning

e) af den dataansvarlige eller databehandleren at få adgang til alle personoplysninger og oplysninger, der er nødvendige for at varetage dens opgaver

f) at få adgang til alle lokaler hos den dataansvarlige og databehandleren, herunder til databehandlingsudstyr og -midler, i overensstemmelse med retsplejeregler i EU-retten eller medlemsstaternes nationale ret.

2. Hver tilsynsmyndighed har alle af følgende korrigerende beføjelser:

a) at udstede advarsler til en dataansvarlig eller en databehandler om, at planlagte behandlingsaktiviteter sandsynligvis vil være i strid med denne forordning

b) at udtale kritik af en dataansvarlig eller en databehandler, hvis behandlingsaktiviteter har været i strid med denne forordning

c) at give den dataansvarlige eller databehandleren påbud om at imødekomme den registreredes anmodninger om at udøve sine rettigheder i henhold til denne forordning

d) at give den dataansvarlige eller databehandleren påbud om at bringe behandlingsaktiviteter i overensstemmelse med bestemmelserne i denne forordning og, hvis det er hensigtsmæssigt, på en nærmere angivet måde og inden for en nærmere angivet frist

e) at give den dataansvarlige påbud om at underrette den registrerede om et brud på persondatasikkerheden

f) midlertidigt eller definitivt at begrænse, herunder forbyde, behandling

g) at give påbud om berigtigelse eller sletning af personoplysninger eller begrænsning af behandling i henhold til artikel 16, 17 og 18 og meddelelse af sådanne handlinger til de modtagere, som personoplysningerne er videregivet til i henhold til artikel 17, stk. 2, og artikel 19

h) at trække en certificering tilbage eller at give et certificeringsorgan påbud om at trække en certificering, der er udstedt i henhold til artikel 42 og 43, tilbage eller at give certificeringsorganet påbud om ikke at udstede en certificering, hvis kravene til certificering ikke er eller ikke længere er opfyldt

i) at pålægge en administrativ bøde i henhold til artikel 83 i tillæg til eller i stedet for foranstaltningerne i dette stykke, afhængigt af omstændighederne i hvert enkelt tilfælde, og

j) at påbyde suspension af overførsel af oplysninger til en modtager i et tredjeland eller til en international organisation.

3. Hver tilsynsmyndighed har alle af følgende godkendelses- og rådgivningsbeføjelser:

a) at rådgive den dataansvarlige efter den procedure for forudgående høring, der er omhandlet i artikel 36

b) på eget initiativ eller på anmodning at afgive udtalelser til det nationale parlament, medlemsstatens regering eller i overensstemmelse med medlemsstaternes nationale ret til andre institutioner og organer samt offentligheden om ethvert spørgsmål om beskyttelse af personoplysninger

c) at godkende den i artikel 36, stk. 5, omhandlede behandling, hvis en sådan forudgående godkendelse er påkrævet i henhold til den pågældende medlemsstats nationale ret

d) at afgive udtalelse og godkende forslag til adfærdskodekser i henhold til artikel 40, stk. 5

e) at akkreditere certificeringsorganer i henhold til artikel 43

f) at udstede certificeringer og godkende kriterier for certificering i overensstemmelse med artikel 42, stk. 5

g) at vedtage standardbestemmelser om databeskyttelse som omhandlet i artikel 28, stk. 8, og i artikel 46, stk. 2, litra d)

h) at godkende kontraktbestemmelser som omhandlet i artikel 46, stk. 3, litra a)

i) at godkende administrative ordninger som omhandlet i artikel 46, stk. 3, litra b)

j) at godkende bindende virksomhedsregler i henhold til artikel 47.

4. Udøvelse af de beføjelser, der tillægges tilsynsmyndigheden i medfør af denne artikel, er underlagt de fornødne garantier, herunder effektive retsmidler og retfærdig procedure, der er fastsat i EU-retten eller medlemsstaternes nationale ret i overensstemmelse med chartret.

5. Hver medlemsstat fastsætter ved lov, at dens tilsynsmyndighed har beføjelse til at indbringe overtrædelser af denne forordning for de judicielle myndigheder og om nødvendigt at indlede eller på anden måde deltage i retssager med henblik på at håndhæve bestemmelserne i denne forordning.

6. Hver medlemsstat kan ved lov fastsætte, at dens tilsynsmyndighed har yderligere beføjelser end dem, der er omhandlet i stk. 1, 2 og 3. Udøvelsen af disse beføjelser må ikke hindre en effektiv anvendelse af kapitel VII.

Artikel 59

Aktivitetsrapport

Hver tilsynsmyndighed udarbejder en årlig rapport om sin virksomhed, eventuelt med en liste over, hvilke typer overtrædelser der er blevet anmeldt, og hvilke typer foranstaltninger der er truffet i henhold til artikel 58, stk. 2. Disse rapporter fremsendes til det nationale parlament, regeringen og andre myndigheder, der er udpeget efter medlemsstaternes nationale ret. De gøres tilgængelige for offentligheden, Kommissionen og Databeskyttelsesrådet.

KAPITEL VII

Samarbejde og sammenhæng

Afdeling 1

Samarbejde

Artikel 60

Samarbejde mellem den ledende tilsynsmyndighed og de andre berørte tilsynsmyndigheder

1. Den ledende tilsynsmyndighed samarbejder i henhold til denne artikel med de andre berørte tilsynsmyndigheder med henblik på at nå til enighed. Den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder udveksler alle relevante oplysninger med hinanden.

2. Den ledende tilsynsmyndighed kan til enhver tid anmode andre berørte tilsynsmyndigheder om at yde gensidig bistand i henhold til artikel 61 og kan gennemføre fælles aktiviteter i henhold til artikel 62, navnlig med henblik på at foretage undersøgelser eller overvåge gennemførelsen af en foranstaltning vedrørende en dataansvarlig eller en databehandler, der er etableret i en anden medlemsstat.

3. Den ledende tilsynsmyndighed underretter straks de andre berørte tilsynsmyndigheder om sagens relevante oplysninger. Den forelægger straks de andre berørte tilsynsmyndigheder et udkast til afgørelse med henblik på deres udtalelse og tager behørigt hensyn til deres synspunkter.

4. Hvis en af de andre berørte tilsynsmyndigheder inden for fire uger efter at være blevet hørt, jf. denne artikels stk. 3, fremkommer med en relevant og begrundet 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.

5. Agter den ledende tilsynsmyndighed at følge den relevante og begrundede indsigelse, forelægger den de andre berørte tilsynsmyndigheder et revideret udkast til afgørelse med henblik på deres udtalelse. Dette reviderede udkast til afgørelse er underlagt den i stk. 4 omhandlede procedure inden for en frist på to uger.

6. Har ingen af de andre berørte tilsynsmyndigheder gjort indsigelse mod udkastet til afgørelse, som den ledende tilsynsmyndighed har forelagt inden for den frist, der er omhandlet i stk. 4 og 5, anses den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder for at være enige i dette udkast til afgørelse og er bundet af det.

7. Den ledende tilsynsmyndighed vedtager og meddeler afgørelsen til den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering, alt efter omstændighederne, og underretter de andre berørte tilsynsmyndigheder og Databeskyttelsesrådet om den pågældende afgørelse, herunder et resumé af de relevante faktiske omstændigheder og begrundelser. Den tilsynsmyndighed, til hvilken der er indgivet klage, underretter klageren om afgørelsen.

8. Hvis en klage er blevet afslået eller afvist, vedtager den tilsynsmyndighed, til hvilken klagen er indgivet, uanset stk. 7, afgørelsen og meddeler denne til klageren og underretter den dataansvarlige herom.

9. Hvis den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder er enige om at afslå eller afvise dele af en klage og at behandle andre dele af klagen, vedtages der en særskilt afgørelse for hver af disse dele af sagen. Den ledende tilsynsmyndighed vedtager afgørelsen for den del, der vedrører foranstaltninger over for den dataansvarlige, meddeler dette til den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering på dens medlemsstats område og underretter klageren herom, mens tilsynsmyndigheden for klageren vedtager afgørelsen for den del, der vedrører afslag eller afvisning af klagen, og underretter klageren herom og meddeler dette til den dataansvarlige eller databehandleren.

10. Den dataansvarlige eller databehandleren træffer efter at være blevet underrettet om den ledende tilsynsmyndigheds afgørelse i henhold til stk. 7 og 9 de nødvendige foranstaltninger til at sikre overholdelse af afgørelsen for så vidt angår behandlingsaktiviteter i forbindelse med alle vedkommendes etableringer i Unionen. Den dataansvarlige eller databehandleren underretter den ledende tilsynsmyndighed, der underretter de andre berørte tilsynsmyndigheder, om de foranstaltninger, der er truffet for at overholde afgørelsen.

11. Hvis en berørt tilsynsmyndighed under ekstraordinære omstændigheder har grund til at mene, at det er nødvendigt at handle omgående for at beskytte registreredes interesser, finder den i artikel 66 omhandlede hasteprocedure anvendelse.

12. Den ledende tilsynsmyndighed og de andre berørte tilsynsmyndigheder udveksler elektronisk de i denne artikel omhandlede oplysninger med hinanden i et standardformat.

Artikel 61

Gensidig bistand

1. Tilsynsmyndighederne udveksler relevante oplysninger og yder hinanden gensidig bistand med henblik på at gennemføre og anvende denne forordning på en ensartet måde og træffer foranstaltninger med henblik på et effektivt samarbejde med hinanden. Gensidig bistand omfatter navnlig anmodninger om oplysninger og tilsynsforanstaltninger, som f.eks. anmodninger om gennemførelse af forudgående godkendelser og høringer, inspektioner og undersøgelser.

2. Hver tilsynsmyndighed træffer alle passende foranstaltninger, som er nødvendige for at besvare en anmodning fra en anden tilsynsmyndighed uden unødig forsinkelse og senest en måned efter modtagelsen af anmodningen. Sådanne foranstaltninger kan bl.a. omfatte videregivelse af relevante oplysninger om gennemførelsen af en undersøgelse.

3. Anmodninger om bistand skal indeholde alle nødvendige oplysninger, herunder formålet med og grunden til anmodningen. Udvekslede oplysninger må kun anvendes til det formål, som er angivet i anmodningen.

4. Den anmodede tilsynsmyndighed må ikke afvise at imødekomme anmodningen, medmindre:

a) den ikke har kompetence med hensyn til genstanden for anmodningen eller de foranstaltninger, som den anmodes om at iværksætte, eller

b) imødekommelse af anmodningen ville udgøre en overtrædelse af denne forordning eller af EU-ret eller medlemsstaternes nationale ret, som den tilsynsmyndighed, der modtager anmodningen, er underlagt.

5. Den anmodede tilsynsmyndighed underretter den anmodende tilsynsmyndighed om resultaterne eller efter omstændighederne om fremskridtene med de foranstaltninger, der er truffet for at imødekomme anmodningen. Den anmodede tilsynsmyndighed begrunder enhver afvisning af at imødekomme en anmodning i henhold til stk. 4.

6. Anmodede tilsynsmyndigheder fremsender som hovedregel de oplysninger, som andre tilsynsmyndigheder anmoder om, elektronisk i et standardformat.

7. Anmodede tilsynsmyndigheder må ikke opkræve gebyr for foranstaltninger, der træffes af dem på grundlag af en anmodning om gensidig bistand. Tilsynsmyndighederne kan vedtage regler om at godtgøre hinanden for specifikke udgifter, der opstår under ekstraordinære omstændigheder, når der ydes gensidig bistand.

8. Hvis en tilsynsmyndighed ikke giver de oplysninger, der er omhandlet i denne artikels stk. 5, inden for en måned efter modtagelsen af en anmodning fra en anden tilsynsmyndighed, kan den anmodende tilsynsmyndighed vedtage en foreløbig foranstaltning på sin medlemsstats område i henhold til artikel 55, stk. 1. I dette tilfælde antages kravet om behovet for at handle omgående, jf. artikel 66, stk. 1, at være opfyldt, og at kræve en hurtig bindende afgørelse fra Databeskyttelsesrådet, jf. artikel 66, stk. 2.

9. Kommissionen kan ved gennemførelsesretsakter fastlægge format og procedurer for gensidig bistand som omhandlet i denne artikel og ordninger for elektronisk udveksling af oplysninger mellem tilsynsmyndigheder og mellem tilsynsmyndigheder og Databeskyttelsesrådet, navnlig standardformatet omhandlet i denne artikels stk. 6. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

Artikel 62

Tilsynsmyndigheders fælles aktiviteter

1. Hvis det er hensigtsmæssigt, gennemfører tilsynsmyndighederne fælles aktiviteter, herunder fælles undersøgelses- og håndhævelsesforanstaltninger, som medlemmer eller medarbejdere fra andre medlemsstaters tilsynsmyndigheder deltager i.

2. Hvis den dataansvarlige eller databehandleren har etableringer i flere medlemsstater, eller hvor et betydeligt antal registrerede i mere end én medlemsstat sandsynligvis påvirkes i væsentlig grad af behandlingsaktiviteter, har tilsynsmyndigheden i hver af disse medlemsstater ret til at deltage i fælles aktiviteter. Den tilsynsmyndighed, der er kompetent i henhold til artikel 56, stk. 1 eller 4, indbyder tilsynsmyndigheden i hver af disse medlemsstater til at deltage i de fælles aktiviteter og besvarer straks en tilsynsmyndigheds anmodning om deltagelse.

3. En tilsynsmyndighed kan i overensstemmelse med medlemsstatens nationale ret og med den udsendende tilsynsmyndigheds godkendelse delegere beføjelser, herunder undersøgelsesbeføjelser, til den udsendende tilsynsmyndigheds medlemmer eller medarbejdere, som deltager i fælles aktiviteter, eller, for så vidt national ret i værtstilsynsmyndighedens medlemsstat tillader det, tillade, at den udsendende tilsynsmyndigheds medlemmer eller medarbejdere udøver deres undersøgelsesbeføjelser i overensstemmelse med retten i den udsendende tilsynsmyndigheds medlemsstat. Sådanne undersøgelsesbeføjelser må kun udøves under vejledning og i tilstedeværelse af værtstilsynsmyndighedens medlemmer eller medarbejdere. Den udsendende tilsynsmyndigheds medlemmer eller medarbejdere er underlagt national ret i værtstilsynsmyndighedens medlemsstat.

4. Hvis en udsendende tilsynsmyndigheds medarbejdere i henhold til stk. 1 udfører aktiviteter i en anden medlemsstat, påtager værtstilsynsmyndighedens medlemsstat sig ansvaret for deres handlinger, herunder erstatningsansvar for enhver skade, som de måtte forvolde under udførelsen af deres aktiviteter, i overensstemmelse med retten i den medlemsstat, på hvis område de udfører aktiviteter.

5. Den medlemsstat, på hvis område skade forvoldes, erstatter den pågældende skade på samme betingelser som skader forvoldt af dens egne medarbejdere. Den udsendende tilsynsmyndigheds medlemsstat, hvis medarbejdere har forvoldt skade på personer på en anden medlemsstats område, skal fuldt ud godtgøre alle beløb, som denne anden medlemsstat har betalt i skadeserstatning til de berettigede personer på deres vegne.

6. Uden at det berører udøvelsen af rettigheder over for tredjemand og med undtagelse af det i stk. 5 omhandlede tilfælde, giver den enkelte medlemsstat i det tilfælde, der er omhandlet i stk. 1, afkald på at kræve godtgørelse fra en anden medlemsstat i forbindelse med skade som omhandlet i stk. 4.

7. Hvis der planlægges en fælles aktivitet, og en tilsynsmyndighed ikke opfylder forpligtelsen i stk. 2, andet punktum, inden for en måned, kan de andre tilsynsmyndigheder vedtage en foreløbig foranstaltning på deres medlemsstats område i overensstemmelse med artikel 55. I dette tilfælde antages kravet om behovet for at handle omgående, jf. artikel 66, stk. 1, at være opfyldt, og at kræve en hurtig bindende afgørelse fra Databeskyttelsesrådet, jf. artikel 66, stk. 2.

Afdeling 2

Sammenhæng

Artikel 63

Sammenhængsmekanisme

Med henblik på at bidrage til en ensartet anvendelse af denne forordning i hele Unionen samarbejder tilsynsmyndighederne med hinanden og, hvis det er relevant, med Kommissionen gennem den sammenhængsmekanisme, der er omhandlet i denne afdeling.

Artikel 64

Udtalelse fra Databeskyttelsesrådet

1. Databeskyttelsesrådet afgiver en udtalelse, når en kompetent tilsynsmyndighed har til hensigt at vedtage en af nedenstående foranstaltninger. Med henblik herpå sender den kompetente tilsynsmyndighed et udkast til afgørelse til Databeskyttelsesrådet, når den:

a) har til hensigt at vedtage en liste over typer af behandlingsaktiviteter, som er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse i henhold til artikel 35, stk. 4

b) behandler et spørgsmål i henhold til artikel 40, stk. 7, om, hvorvidt et udkast til adfærdskodeks eller en ændring eller udvidelse af en adfærdskodeks overholder denne forordning

c) har til hensigt at godkende kriterierne for akkreditering af et organ i henhold til artikel 41, stk. 3, eller et certificeringsorgan i henhold til artikel 43, stk. 3

d) har til hensigt at vedtage standardbestemmelser om databeskyttelse som omhandlet i artikel 46, stk. 2, litra d), og i artikel 28, stk. 8

e) har til hensigt at godkende kontraktbestemmelser som omhandlet i artikel 46, stk. 3, litra a), eller

f) har til hensigt at godkende bindende virksomhedsregler som omhandlet i artikel 47.

2. En tilsynsmyndighed, formanden for Databeskyttelsesrådet eller Kommissionen kan kræve, at ethvert almengyldigt spørgsmål eller ethvert spørgsmål, der har virkninger i mere end én medlemsstat, drøftes af Databeskyttelsesrådet med henblik på en udtalelse, navnlig hvis en kompetent tilsynsmyndighed ikke opfylder forpligtelserne vedrørende gensidig bistand, jf. artikel 61, eller vedrørende fælles aktiviteter, jf. artikel 62.

3. I de tilfælde, der er omhandlet i stk. 1 og 2, afgiver Databeskyttelsesrådet 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 blandt medlemmerne af Databeskyttelsesrådet. Denne frist kan forlænges med yderligere seks uger under hensyntagen til spørgsmålets kompleksitet. Med hensyn til det i stk. 1 omhandlede udkast til afgørelse, der i henhold til stk. 5 udsendes til medlemmerne af Databeskyttelsesrådet, anses et medlem, som ikke har gjort indsigelse inden for en rimelig frist, der angives af formanden, for at være enigt i udkastet til afgørelse.

4. Tilsynsmyndigheder og Kommissionen sender uden unødig forsinkelse elektronisk og i et standardformat Databeskyttelsesrådet alle relevante oplysninger, herunder et resumé af de faktiske omstændigheder, den foreslåede afgørelse, begrundelsen for vedtagelse af en sådan foranstaltning og andre berørte tilsynsmyndigheders synspunkter.

5. Formanden for Databeskyttelsesrådet underretter uden unødig forsinkelse elektronisk:

a) medlemmerne af Databeskyttelsesrådet og Kommissionen om alle relevante oplysninger, som vedkommende har modtaget, i et standardformat. Sekretariatet for Databeskyttelsesrådet sørger efter behov for oversættelse af de relevante oplysninger, og

b) den tilsynsmyndighed, der er omhandlet i stk. 1 og 2, og Kommissionen om den pågældende udtalelse og offentliggør den.

6. Den kompetente tilsynsmyndighed vedtager ikke sit udkast til afgørelse omhandlet i stk. 1 i den periode, der er omhandlet i stk. 3.

7. Den tilsynsmyndighed, der er omhandlet i stk. 1, tager videst muligt hensyn til Databeskyttelsesrådets udtalelse og giver senest to uger efter modtagelsen af udtalelsen 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.

8. Hvis den berørte tilsynsmyndighed inden for den frist, der er omhandlet i denne artikels stk. 7, underretter formanden for Databeskyttelsesrådet om, at den helt eller delvist ikke agter at følge udtalelsen fra Databeskyttelsesrådet, og den giver en relevant begrundelse herfor, finder artikel 65, stk. 1, anvendelse.

Artikel 65

Tvistbilæggelse ved Databeskyttelsesrådet

1. Med henblik på at sikre korrekt og konsekvent anvendelse af denne forordning i hvert enkelt tilfælde vedtager Databeskyttelsesrådet en bindende afgørelse i følgende tilfælde:

a) hvis en berørt tilsynsmyndighed i et tilfælde som omhandlet i artikel 60, stk. 4, er fremkommet med en relevant og begrundet indsigelse mod et udkast til afgørelse udarbejdet af den ledende myndighed, eller den ledende myndighed har afvist en sådan indsigelse som værende uden relevans eller ubegrundet. Den bindende afgørelse skal vedrøre alle spørgsmål, der er genstand for den relevante og begrundede indsigelse, navnlig hvorvidt denne forordning er overtrådt

b) hvis der er uenighed om, hvilken af de berørte tilsynsmyndigheder der er kompetent med hensyn til hovedvirksomheden

c) hvis en kompetent tilsynsmyndighed ikke anmoder om udtalelse fra Databeskyttelsesrådet i de tilfælde, der er omhandlet i artikel 64, stk. 1, eller ikke følger Databeskyttelsesrådets udtalelse udstedt i henhold til artikel 64. I så fald kan enhver berørt tilsynsmyndighed eller Kommissionen indbringe spørgsmålet for Databeskyttelsesrådet.

2. Den afgørelse, der er omhandlet i stk. 1, vedtages inden for en måned fra forelæggelsen af spørgsmålet med et flertal på to tredjedele blandt medlemmerne af Databeskyttelsesrådet. Denne frist kan forlænges med yderligere en måned på grund af spørgsmålets kompleksitet. Afgørelsen i stk. 1 skal være begrundet og rettet til den ledende tilsynsmyndighed og alle de berørte tilsynsmyndigheder og have bindende virkning for dem.

3. Hvis Databeskyttelsesrådet ikke har været i stand til at træffe en afgørelse inden for de i stk. 2 omhandlede frister, vedtager det sin afgørelse senest to uger efter udløbet af den anden måned som omhandlet i stk. 2 med simpelt flertal blandt Databeskyttelsesrådets medlemmer. I tilfælde af stemmelighed blandt medlemmerne af Databeskyttelsesrådet er formandens stemme udslagsgivende.

4. De berørte tilsynsmyndigheder må ikke vedtage en afgørelse om et spørgsmål, der er forelagt for Databeskyttelsesrådet i henhold til stk. 1, i løbet af de i stk. 2 og 3 omhandlede perioder.

5. Formanden for Databeskyttelsesrådet meddeler uden unødig forsinkelse den i stk. 1 omhandlede afgørelse til de berørte tilsynsmyndigheder. Formanden underretter Kommissionen herom. Afgørelsen offentliggøres straks på Databeskyttelsesrådets websted, når tilsynsmyndigheden har meddelt den endelige afgørelse, jf. stk. 6.

6. Den ledende tilsynsmyndighed eller efter omstændighederne den tilsynsmyndighed, til hvem en klage er indgivet, vedtager sin endelige afgørelse på grundlag af den i denne artikels stk. 1 omhandlede afgørelse uden unødig forsinkelse og senest en måned efter, at Databeskyttelsesrådet har meddelt sin afgørelse. Den ledende tilsynsmyndighed eller efter omstændighederne den tilsynsmyndighed, til hvem klagen er indgivet, underretter Databeskyttelsesrådet om datoen for meddelelse af sin endelige afgørelse til henholdsvis den dataansvarlige eller databehandleren og den registrerede. Den berørte tilsynsmyndigheds endelige afgørelse vedtages i henhold til artikel 60, stk. 7, 8 og 9. Den endelige afgørelse skal indeholde en henvisning til den afgørelse, der er omhandlet i nærværende artikels stk. 1, og angive, at den i nævnte stykke omhandlede afgørelse vil blive offentliggjort på Databeskyttelsesrådets websted i overensstemmelse med nærværende artikels stk. 5. Den i nærværende artikels stk. 1 omhandlede afgørelse vedlægges den endelige afgørelse.

Artikel 66

Hasteprocedure

1. Når en berørt tilsynsmyndighed under ekstraordinære omstændigheder mener, at det er nødvendigt at handle omgående for at beskytte registreredes rettigheder og frihedsrettigheder, kan den uanset den i artikel 63, 64 og 65 omhandlede sammenhængsmekanisme eller den i artikel 60 omhandlede procedure omgående træffe foreløbige foranstaltninger, der skal have retsvirkning på dens eget område med en angivet gyldighedsperiode, som ikke må overstige tre måneder. Tilsynsmyndigheden meddeler straks de andre berørte tilsynsmyndigheder, Databeskyttelsesrådet og Kommissionen disse foranstaltninger og en begrundelse for vedtagelsen heraf.

2. Hvis en tilsynsmyndighed har vedtaget en foranstaltning i henhold til stk. 1 og mener, at der omgående skal vedtages endelige foranstaltninger, kan den anmode om en hasteudtalelse eller en hurtig bindende afgørelse fra Databeskyttelsesrådet, idet tilsynsmyndigheden begrunder anmodningen om en sådan udtalelse eller afgørelse.

3. Enhver tilsynsmyndighed kan anmode om en hasteudtalelse eller efter omstændighederne en hurtig bindende afgørelse, fra Databeskyttelsesrådet, hvis en kompetent tilsynsmyndighed ikke har truffet de fornødne foranstaltninger i en situation, hvor det er nødvendigt at handle omgående for at beskytte registreredes rettigheder og frihedsrettigheder, idet tilsynsmyndigheden begrunder anmodningen om en sådan udtalelse eller afgørelse, herunder behovet for at handle omgående.

4. Uanset artikel 64, stk. 3, og artikel 65, stk. 2, vedtages en hasteudtalelse eller en hurtig bindende afgørelse som omhandlet i nærværende artikels stk. 2 og 3 inden for to uger med simpelt flertal blandt medlemmerne af Databeskyttelsesrådet.

Artikel 67

Udveksling af oplysninger

Kommissionen kan vedtage gennemførelsesretsakter af generel karakter med henblik på nærmere at angive ordningerne for elektronisk udveksling af oplysninger mellem tilsynsmyndigheder og mellem tilsynsmyndigheder og Databeskyttelsesrådet, navnlig det standardformat, der er omhandlet i artikel 64.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

Afdeling 3

Det Europæiske Databeskyttelsesråd

Artikel 68

Det Europæiske Databeskyttelsesråd

1. Det Europæiske Databeskyttelsesråd (»Databeskyttelsesrådet«) oprettes herved som et EU-organ med status som juridisk person.

2. Databeskyttelsesrådet repræsenteres af sin formand.

3. Databeskyttelsesrådet sammensættes af chefen for en tilsynsmyndighed i hver medlemsstat og af Den Europæiske Tilsynsførende for Databeskyttelse eller deres respektive repræsentanter.

4. Hvis mere end én tilsynsmyndighed i en medlemsstat er ansvarlig for at føre tilsyn med af anvendelsen af bestemmelserne i denne forordning, udnævnes en fælles repræsentant i henhold til den pågældende medlemsstats nationale ret.

5. Kommissionen har ret til at deltage i Databeskyttelsesrådets aktiviteter og møder uden stemmeret. Kommissionen udpeger en repræsentant. Formanden for Databeskyttelsesrådet underretter Kommissionen om aktiviteterne i Databeskyttelsesrådet.

6. I de i artikel 65 omhandlede tilfælde har Den Europæiske Tilsynsførende for Databeskyttelse kun stemmeret i forbindelse med afgørelser, der vedrører principper og bestemmelser, som gælder for Unionens institutioner, organer, kontorer og agenturer, og som indholdsmæssigt er i overensstemmelse med denne forordnings principper og bestemmelser.

Artikel 69

Uafhængighed

1. Databeskyttelsesrådet handler uafhængigt, når det udfører sine opgaver eller udøver sine beføjelser i henhold til artikel 70 og 71.

2. Uden at det berører anmodninger fra Kommissionen som omhandlet i artikel 70, stk. 1, litra b), og stk. 2, må Databeskyttelsesrådet ikke søge eller modtage instrukser fra andre i forbindelse med udførelsen af sine opgaver eller udøvelsen af sine beføjelser.

Artikel 70

Databeskyttelsesrådets opgaver

1. Databeskyttelsesrådet sikrer ensartet anvendelse af denne forordning. Med henblik herpå skal Databeskyttelsesrådet på eget initiativ eller, når det er relevant, efter anmodning fra Kommissionen navnlig:

a) føre tilsyn med og sikre korrekt anvendelse af denne forordning i de tilfælde, der er omhandlet i artikel 64 og 65, uden at dette berører de nationale tilsynsmyndigheders opgaver

b) rådgive Kommissionen om ethvert spørgsmål vedrørende beskyttelse af personoplysninger i Unionen, herunder om ethvert forslag til ændring af denne forordning

c) rådgive Kommissionen om format og procedurer for videregivelse af oplysninger mellem dataansvarlige, databehandlere og tilsynsmyndigheder vedrørende bindende virksomhedsregler

d) udstede retningslinjer, henstillinger og bedste praksis vedrørende procedurer for sletning af link til og kopier eller gengivelser af personoplysninger fra offentligt tilgængelige kommunikationstjenester som omhandlet i artikel 17, stk. 2

e) på eget initiativ, efter anmodning fra et af sine medlemmer eller efter anmodning fra Kommissionen undersøge ethvert spørgsmål vedrørende anvendelsen af denne forordning og udstede retningslinjer, henstillinger og bedste praksis for at fremme ensartet anvendelse af denne forordning

f) udstede retningslinjer, henstillinger og bedste praksis i overensstemmelse med dette stykkes litra e) med henblik på nærmere at angive kriterierne og betingelserne for afgørelser baseret på profilering i henhold til artikel 22, stk. 2

g) udstede retningslinjer, henstillinger og bedste praksis i overensstemmelse med dette stykkes litra e) med henblik på 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

h) udstede retningslinjer, henstillinger og bedste praksis i overensstemmelse med dette stykkes litra e) vedrørende 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

i) udstede retningslinjer, henstillinger og bedste praksis i overensstemmelse med dette stykkes litra e) med henblik på nærmere at angive kriterierne for og kravene til overførsel af personoplysninger baseret på bindende virksomhedsregler, som dataansvarlige overholder, og bindende virksomhedsregler, som databehandlere overholder, og vedrørende yderligere krav til at sikre beskyttelse af de berørte registreredes personoplysninger som omhandlet i artikel 47

j) udstede retningslinjer, henstillinger og bedste praksis i overensstemmelse med dette stykkes litra e) med henblik på nærmere at angive kriterierne for og kravene til overførsel af personoplysninger på grundlag af artikel 49, stk. 1

k) udarbejde retningslinjer for tilsynsmyndighederne vedrørende anvendelse af foranstaltninger, jf. artikel 58, stk. 1, 2 og 3, og fastsættelse af administrative bøder i henhold til artikel 83

l) gennemgå den praktiske anvendelse af de retningslinjer og henstillinger og den bedste praksis, der er omhandlet i litra e) og f)

m) udstede retningslinjer, henstillinger og bedste praksis i overensstemmelse med dette stykkes litra e) med henblik på fastlæggelse af fælles procedurer for fysiske personers indberetning af overtrædelser af denne forordning, jf. artikel 54, stk. 2,

n) tilskynde til udarbejdelse af adfærdskodekser og fastlæggelse af certificeringsmekanismer for databeskyttelse og databeskyttelsesmærkninger og -mærker i henhold til artikel 40 og 42

o) foretage akkreditering af certificeringsorganer og regelmæssig revision heraf i henhold til artikel 43 og føre et offentligt register over akkrediterede organer i henhold til artikel 43, stk. 6, og over de akkrediterede dataansvarlige eller databehandlere i tredjelande i henhold til artikel 42, stk. 7

p) angive de krav, der er omhandlet i artikel 43, stk. 3, med henblik på akkreditering af certificeringsorganer i henhold til artikel 42

q) afgive udtalelse til Kommissionen om de certificeringskrav, der er omhandlet i artikel 43, stk. 8

r) afgive udtalelse til Kommissionen om de ikoner, der er omhandlet i artikel 12, stk. 7

s) afgive udtalelse til Kommissionen med henblik på vurdering af tilstrækkeligheden af beskyttelsesniveauet i et tredjeland eller en international organisation, herunder vurdering af, om et tredjeland, et område eller en eller flere specifikke sektorer i det pågældende tredjeland, eller en international organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau. Til dette formål forelægger Kommissionen Databeskyttelsesrådet al nødvendig dokumentation vedrørende tredjelandet, området eller den specifikke sektor, eller den internationale organisation, herunder korrespondance med regeringen i tredjelandet,

t) afgive udtalelser om tilsynsmyndigheders udkast til afgørelse i overensstemmelse med den sammenhængsmekanisme, der er omhandlet i artikel 64, stk. 1, og om sager, der er forelagt i henhold til artikel 64, stk. 2, og udstede bindende afgørelser i henhold til artikel 65, herunder i de tilfælde, der er omhandlet i artikel 66

u) fremme samarbejdet og effektiv bilateral og multilateral udveksling af oplysninger og bedste praksis mellem tilsynsmyndighederne

v) fremme fælles uddannelsesprogrammer og udveksling af personale mellem tilsynsmyndighederne og i relevante tilfælde med tilsynsmyndighederne i tredjelande eller med internationale organisationer

w) fremme udveksling af viden og dokumentation vedrørende databeskyttelseslovgivning og -praksis med datatilsynsmyndigheder over hele verden

x) afgive udtalelser om adfærdskodekser, der udarbejdes på EU-plan, jf. artikel 40, stk. 9, og

y) føre et offentligt tilgængeligt elektronisk register over afgørelser truffet af tilsynsmyndigheder og domstole om spørgsmål, der er blevet behandlet i sammenhængsmekanismen.

2. Hvis Kommissionen anmoder Databeskyttelsesrådet om rådgivning, kan den fastsætte en frist under hensyntagen til, hvor meget den pågældende sag haster.

3. Databeskyttelsesrådet fremsender sine udtalelser, retningslinjer, henstillinger og bedste praksis til Kommissionen og det udvalg, der er omhandlet i artikel 93, og offentliggør dem.

4. Databeskyttelsesrådet hører efter omstændighederne berørte parter og giver dem mulighed for at fremsætte bemærkninger inden for en rimelig frist. Databeskyttelsesrådet offentliggør med forbehold af artikel 76 resultaterne af høringsproceduren.

Artikel 71

Rapporter

1. Databeskyttelsesrådet udarbejder en årlig rapport om beskyttelse af fysiske personer i forbindelse med behandling i Unionen og, hvis det er relevant, i tredjelande og internationale organisationer. Rapporten offentliggøres og forelægges Europa-Parlamentet, Rådet og Kommissionen.

2. Den årlige rapport skal omfatte en gennemgang af den praktiske anvendelse af de retningslinjer og henstillinger og den bedste praksis, der er omhandlet i artikel 70, stk. 1, litra l), og de bindende afgørelser, der er omhandlet i artikel 65.

Artikel 72

Procedure

1. Databeskyttelsesrådet træffer afgørelse med simpelt flertal blandt sine medlemmer, medmindre andet er fastsat i denne forordning.

2. Databeskyttelsesrådet vedtager sin forretningsorden med et flertal på to tredjedele blandt sine medlemmer og tilrettelægger sin drift.

Artikel 73

Formand

1. Databeskyttelsesrådet vælger med simpelt flertal en formand og to næstformænd blandt sine medlemmer.

2. Embedsperioden for formanden og de to næstformænd er fem år med mulighed for forlængelse én gang.

Artikel 74

Formandens opgaver

1. Formanden har følgende opgaver:

a) at indkalde til møder i Databeskyttelsesrådet og udarbejde dagsordenen herfor

b) at underrette den ledende tilsynsmyndighed og de berørte tilsynsmyndigheder om de afgørelser, der vedtages af Databeskyttelsesrådet i henhold til artikel 65

c) at sikre, at Databeskyttelsesrådets opgaver udføres rettidigt, navnlig i forbindelse med den sammenhængsmekanisme, der er omhandlet i artikel 63.

2. Databeskyttelsesrådet fastlægger fordelingen af opgaver mellem formanden og næstformændene i sin forretningsorden.

Artikel 75

Sekretariat

1. Databeskyttelsesrådet har et sekretariat, som stilles til rådighed af Den Europæiske Tilsynsførende for Databeskyttelse.

2. Sekretariatet udfører udelukkende sine opgaver efter instruks fra formanden for Databeskyttelsesrådet.

3. Det personale ved Den Europæiske Tilsynsførende for Databeskyttelse, der deltager i udførelsen af Databeskyttelsesrådets opgaver i henhold til denne forordning, skal have særskilte rapporteringsveje i forhold til det personale, der deltager i udførelsen af opgaver, som Den Europæiske Tilsynsførende for Databeskyttelse har fået tildelt.

4. Databeskyttelsesrådet og Den Europæiske Tilsynsførende for Databeskyttelse udarbejder og offentliggør om nødvendigt et aftalememorandum til gennemførelse af denne artikel, som fastsætter vilkårene for deres samarbejde, og som gælder for det personale ved Den Europæiske Tilsynsførende for Databeskyttelse, der deltager i udførelsen af Databeskyttelsesrådets opgaver i henhold til denne forordning.

5. Sekretariatet yder analytisk, administrativ og logistisk støtte til Databeskyttelsesrådet.

6. Sekretariatet er navnlig ansvarligt for:

a) Databeskyttelsesrådets daglige arbejde

b) kommunikation mellem medlemmerne af Databeskyttelsesrådet, dets formand og Kommissionen

c) kommunikation med andre institutioner og offentligheden

d) brug af elektroniske midler til intern og ekstern kommunikation

e) oversættelse af relevante oplysninger

f) forberedelse og opfølgning af Databeskyttelsesrådets møder

g) forberedelse, udarbejdelse og offentliggørelse af udtalelser, afgørelser om bilæggelse af tvister mellem tilsynsmyndigheder og andre dokumenter, der vedtages af Databeskyttelsesrådet.

Artikel 76

Fortrolighed

1. Databeskyttelsesrådets drøftelser er fortrolige, hvis Databeskyttelsesrådet vurderer, at det er nødvendigt, jf. dets forretningsorden.

2. Aktindsigt i dokumenter, der forelægges medlemmer af Databeskyttelsesrådet, eksperter og repræsentanter for tredjemand, er omfattet af Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 ([1]).

KAPITEL VIII

Retsmidler, ansvar og sanktioner

Artikel 77

Ret til at indgive klage til en tilsynsmyndighed

1. Uden at det berører andre administrative klageadgange eller adgang til retsmidler, har enhver registreret ret til at indgive klage til en tilsynsmyndighed, navnlig i den medlemsstat, hvor vedkommende har sit sædvanlige opholdssted eller sit arbejdssted, eller hvor den påståede overtrædelse har fundet sted, hvis den registrerede finder, at behandlingen af personoplysninger vedrørende vedkommende overtræder denne forordning.

2. Den tilsynsmyndighed, som klagen er indgivet til, underretter klageren om forløbet og resultatet af klagen, herunder om muligheden for anvendelse af retsmidler, jf. artikel 78.

Artikel 78

Adgang til effektive retsmidler over for en tilsynsmyndighed

1. Uden at det berører andre administrative eller udenretslige klageadgange, har enhver fysisk eller juridisk person ret til effektive retsmidler over for en juridisk bindende afgørelse truffet af en tilsynsmyndighed vedrørende vedkommende.

2. Uden at det berører andre administrative eller udenretslige klageadgange, har den enkelte registrerede adgang til effektive retsmidler, hvis den tilsynsmyndighed, der er kompetent i henhold til artikel 55 og 56, ikke behandler en klage eller undlader at underrette den registrerede om forløbet eller resultatet af en klage, der er indgivet i henhold til artikel 77, inden for tre måneder.

3. En sag mod en tilsynsmyndighed anlægges ved en domstol i den medlemsstat, hvor tilsynsmyndigheden er etableret.

4. Hvis sag anlægges mod en afgørelse fra en tilsynsmyndighed, der er truffet efter en udtalelse eller en afgørelse fra Databeskyttelsesrådet i forbindelse med sammenhængsmekanismen, fremsender tilsynsmyndigheden denne udtalelse eller afgørelse til domstolen.

Artikel 79

Adgang til effektive retsmidler over for en dataansvarlig eller databehandler

1. Uden at det berører andre tilgængelige administrative eller udenretslige klageadgange, herunder retten til at indgive klage til en tilsynsmyndighed i henhold til artikel 77, skal den enkelte registrerede have adgang til effektive retsmidler, hvis vedkommende finder, at vedkommendes rettigheder i henhold til denne forordning er blevet krænket som følge af behandling af vedkommendes personoplysninger i strid med denne forordning.

2. En sag mod en dataansvarlig eller en databehandler anlægges ved en domstol i den medlemsstat, hvor den dataansvarlige eller databehandleren er etableret. Alternativt kan en sådan sag anlægges ved en domstol i den medlemsstat, hvor den registrerede har sit sædvanlige opholdssted, medmindre den dataansvarlige eller databehandleren er en offentlig myndighed i en medlemsstat, der udøver sine offentligretlige beføjelser.

([1]) Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter (EFT L 145 af 31.5.2001, s. 43).

Artikel 80

Repræsentation af registrerede

1. Den registrerede har ret til at bemyndige et organ, en organisation eller en sammenslutning, der er etableret i overensstemmelse med en medlemsstats nationale ret, som ikke arbejder med gevinst for øje, hvis vedtægtsmæssige formål er af almen interesse, og som er aktiv på området for beskyttelse af registreredes rettigheder og frihedsrettigheder med hensyn til beskyttelse af deres personoplysninger, til at indgive en klage på sine vegne, til at udøve de rettigheder, der er omhandlet i artikel 77, 78 og 79, på sine vegne og til, hvis det er fastsat i medlemsstaternes nationale ret, at udøve retten til at modtage erstatning som omhandlet i artikel 82 på sine vegne.

2. Medlemsstaterne kan fastsætte, at ethvert organ, enhver organisation eller enhver sammenslutning, jf. denne artikels stk. 1, uafhængigt af en bemyndigelse fra den registrerede har ret til at indgive en klage i den pågældende medlemsstat til den tilsynsmyndighed, der er kompetent i henhold til artikel 77, og til at udøve de rettigheder, der er omhandlet i artikel 78 og 79, hvis den/det har grund til at formode, at den registreredes rettigheder i henhold til denne forordning er blevet krænket som følge af behandling.

Artikel 81

Udsættelse af en sag

1. Hvis en kompetent domstol i en medlemsstat har oplysninger om, at der verserer en sag vedrørende samme genstand for så vidt angår behandling foretaget af den samme dataansvarlige eller databehandler ved en domstol i en anden medlemsstat, skal den rette henvendelse til pågældende domstol i den anden medlemsstat for at bekræfte eksistensen af en sådan sag.

2. Hvis der verserer en sag vedrørende samme genstand for så vidt angår behandling foretaget af den samme dataansvarlige eller databehandler ved en domstol i en anden medlemsstat, kan enhver anden kompetent domstol end den, ved hvilken sagen først er anlagt, udsætte sagen.

3. Hvis denne sag verserer ved første instans, kan enhver anden domstol end den, ved hvilken sagen først er anlagt, efter anmodning fra en af parterne også erklære sig inkompetent, hvis den domstol, ved hvilken sagen først er anlagt, har kompetence til at behandle de pågældende sager, og forening heraf er tilladt i henhold til dens lovgivning.

Artikel 82

Ret til erstatning og erstatningsansvar

1. Enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren.

2. Enhver dataansvarlig, der er involveret i behandling, hæfter for den skade, der er forvoldt af behandling, der overtræder denne forordning. En databehandler hæfter kun for den skade, der er forvoldt af behandling, hvis pågældende ikke har opfyldt forpligtelser i denne forordning, der er rettet specifikt mod databehandlere, eller hvis pågældende har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser.

3. En dataansvarlig eller databehandler er fritaget for erstatningsansvar i henhold til stk. 2, hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden.

4. Hvis mere end én dataansvarlig eller databehandler eller både en dataansvarlig og en databehandler er involveret i den samme behandling, og hvis de i henhold til stk. 2 og 3 er ansvarlige for skader, der er forvoldt af behandling, hæfter de solidarisk for hele skaden for at sikre fuld erstatning til den registrerede.

5. Hvis en dataansvarlig eller en databehandler i overensstemmelse med stk. 4 har betalt fuld erstatning for den forvoldte skade, har den pågældende dataansvarlige eller databehandler ret til at kræve den del af erstatningen, der svarer til andres del af ansvaret for skaden, tilbage fra de andre dataansvarlige eller databehandlere, der er involveret i den samme behandling, i overensstemmelse med betingelserne i stk. 2.

6. Retssager med henblik på udøvelse af retten til at modtage erstatning anlægges ved de domstole, der er kompetente i henhold til national ret i den medlemsstat, der er omhandlet i artikel 79, stk. 2.

Artikel 83

Generelle betingelser for pålæggelse af administrative bøder

1. Hver tilsynsmyndighed sikrer, at pålæggelse af administrative bøder i henhold til denne artikel for overtrædelse af denne forordning som omhandlet i stk. 4, 5 og 6 i hver enkelt sag er effektiv, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning.

2. Afhængigt af omstændighederne i hver enkelt sag pålægges administrative bøder i tillæg til eller i stedet for foranstaltninger som omhandlet i artikel 58, stk. 2, litra a)-h) og j). Når der træffes afgørelse om, hvorvidt der skal pålægges en administrativ bøde, og om den administrative bødes størrelse i hver enkelt sag, tages der behørigt hensyn til følgende:

a) overtrædelsens karakter, alvor og varighed under hensyntagen til pågældende behandlings karakter, omfang eller formål samt antal registrerede, der er berørt, og omfanget af den skade, som de har lidt

b) hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt

c) eventuelle foranstaltninger, der er truffet af den dataansvarlige eller databehandleren for at begrænse den skade, som den registrerede har lidt

d) den dataansvarliges eller databehandlerens grad af ansvar under hensyntagen til tekniske og organisatoriske foranstaltninger, som de har gennemført i henhold til artikel 25 og 32

e) den dataansvarliges eller databehandlerens eventuelle relevante tidligere overtrædelser

f) graden af samarbejde med tilsynsmyndigheden for at afhjælpe overtrædelsen og begrænse de negative konsekvenser, som overtrædelsen måtte have givet anledning til

g) de kategorier af personoplysninger, der er berørt af overtrædelsen

h) den måde, hvorpå tilsynsmyndigheden fik kendskab til overtrædelsen, navnlig om den dataansvarlige eller databehandleren har underrettet om overtrædelsen, og i givet fald i hvilket omfang

i) overholdelse af de foranstaltninger, der er omhandlet i artikel 58, stk. 2, hvis der tidligere over for den pågældende dataansvarlige eller databehandler er blevet truffet sådanne foranstaltninger med hensyn til samme genstand

j) overholdelse af godkendte adfærdskodekser i henhold til artikel 40 eller godkendte certificeringsmekanismer i henhold til artikel 42, og

k) om der er andre skærpende eller formildende faktorer ved sagens omstændigheder, såsom opnåede økonomiske fordele eller undgåede tab som direkte eller indirekte følge af overtrædelsen.

3. Hvis en dataansvarlig eller en databehandler forsætligt eller uagtsomt i forbindelse med de samme eller forbundne behandlingsaktiviteter overtræder flere bestemmelser i denne forordning, må den administrative bødes samlede størrelse ikke overstige beløbet for den alvorligste overtrædelse.

4. Overtrædelse af følgende bestemmelser straffes i overensstemmelse med stk. 2 med administrative bøder på op til 10 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 2 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere:

a) den dataansvarliges og databehandlerens forpligtelser i henhold til artikel 8, 11, 25-39 og 42 og 43

b) certificeringsorganets forpligtelser i henhold til artikel 42 og 43

c) kontrolorganets forpligtelser i henhold til artikel 41, stk. 4.

5. Overtrædelse af følgende bestemmelser straffes i overensstemmelse med stk. 2 med administrative bøder på op til 20 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere:

a) de grundlæggende principper for behandling, herunder betingelserne for samtykke, i artikel 5, 6, 7 og 9

b) de registreredes rettigheder i henhold til artikel 12-22

c) overførsel af personoplysninger til en modtager i et tredjeland eller en international organisation i henhold til artikel 44-49

d) eventuelle forpligtigelser i medfør af medlemsstaternes nationale ret vedtaget i henhold til kapitel IX

e) manglende overholdelse af et påbud eller en midlertidig eller definitiv begrænsning af behandling eller tilsynsmyndighedens suspension af overførsel af oplysninger i henhold til artikel 58, stk. 2, eller manglende adgang i strid med artikel 58, stk. 1.

6. Manglende overholdelse af et påbud fra tilsynsmyndigheden som omhandlet i artikel 58, stk. 2, straffes i overensstemmelse med nærværende artikels stk. 2 med administrative bøder på op til 20 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere.

7. Uden at det berører tilsynsmyndighedernes korrigerende beføjelser i henhold til artikel 58, stk. 2, kan hver medlemsstat fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat.

8. Tilsynsmyndighedens udøvelse af beføjelser i henhold til denne artikel skal være underlagt fornødne proceduremæssige garantier i overensstemmelse med EU-retten og medlemsstaternes nationale ret, bl.a. effektive retsmidler og retfærdig procedure.

9. Hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, kan denne artikel anvendes på en sådan måde, at den kompetente tilsynsmyndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af tilsynsmyndighederne. Bøder skal under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. De pågældende medlemsstater giver Kommissionen meddelelse om bestemmelserne i deres love, som de vedtager i henhold til dette stykke, senest den 25. maj 2018 og underretter den straks om alle senere ændringslove eller ændringer, der berører dem.

Artikel 84

Sanktioner

1. Medlemsstaterne fastsætter regler om andre sanktioner, der skal anvendes i tilfælde af overtrædelser af denne forordning, navnlig overtrædelser, som ikke er underlagt administrative bøder i henhold til artikel 83, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

2. Hver medlemsstat giver senest den 25. maj 2018 Kommissionen meddelelse om de bestemmelser, som den vedtager i henhold til stk. 1, og underretter den straks om alle senere ændringer, der berører dem.

KAPITEL IX

Bestemmelser vedrørende specifikke behandlingssituationer

Artikel 85

Behandling og ytrings- og informationsfriheden

1. Medlemsstaterne forener ved lov retten til beskyttelse af personoplysninger i henhold til denne forordning med retten til ytrings- og informationsfrihed, herunder behandling i journalistisk øjemed og med henblik på akademisk, kunstnerisk eller litterær virksomhed.

2. Til behandling i journalistisk øjemed eller med henblik på akademisk, kunstnerisk eller litterær virksomhed fastsætter medlemsstaterne undtagelser eller fravigelser fra kapitel II (principper), kapitel III (den registreredes rettigheder), kapitel IV (dataansvarlig og databehandler), kapitel V (overførsel af personoplysninger til tredjelande eller internationale organisationer), kapitel VI (uafhængige tilsynsmyndigheder), kapitel VII (samarbejde og sammenhæng) og kapitel IX (specifikke databehandlingssituationer), hvis de er nødvendige for at forene retten til beskyttelse af personoplysninger med ytrings- og informationsfriheden.

3. Hver medlemsstat giver Kommissionen meddelelse om de lovbestemmelser, som den har vedtaget i henhold til stk. 2, og underretter den straks om alle senere ændringslove eller ændringer, der berører dem.

Artikel 86

Behandling og aktindsigt i officielle dokumenter

Personoplysninger i officielle dokumenter, som en offentlig myndighed eller et offentligt eller privat organ er i besiddelse af med henblik på udførelse af en opgave i samfundets interesse, må videregives af myndigheden eller organet i overensstemmelse med EU-retten eller medlemsstaternes nationale ret, som den offentlige myndighed eller organet er underlagt, for at forene aktindsigt i officielle dokumenter med retten til beskyttelse af personoplysninger i henhold til denne forordning.

Artikel 87

Behandling af nationalt identifikationsnummer

Medlemsstaterne kan nærmere 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.

Artikel 88

Behandling i forbindelse med ansættelsesforhold

1. Medlemsstaterne kan ved lov eller i medfør af kollektive overenskomster fastsætte mere specifikke bestemmelser for at sikre beskyttelse af rettighederne og frihedsrettighederne i forbindelse med behandling af arbejdstageres personoplysninger i ansættelsesforhold, navnlig med henblik på ansættelse, ansættelseskontrakter, herunder opfyldelse af forpligtelser fastsat ved lov eller i kollektive overenskomster, ledelse, planlægning og tilrettelæggelse af arbejdet, ligestilling og mangfoldighed på arbejdspladsen, arbejdsmiljø samt beskyttelse af arbejdsgiveres eller kunders ejendom og med henblik på individuel eller kollektiv udøvelse og nydelse af rettigheder og fordele i forbindelse med ansættelse samt med henblik på ophør af ansættelsesforhold.

2. Disse bestemmelser skal omfatte passende og specifikke foranstaltninger til beskyttelse af den registreredes menneskelige værdighed, legitime interesser og grundlæggende rettigheder, særlig med hensyn til gennemsigtighed i behandlingen, overførsel af personoplysninger inden for en koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet, og overvågningssystemer på arbejdspladsen.

3. Hver medlemsstat giver senest den 25. maj 2018 Kommissionen meddelelse om de bestemmelser, som den vedtager i henhold til stk. 1, og underretter den straks om alle senere ændringer, der berører dem.

Artikel 89

Garantier og undtagelser i forbindelse med behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål

1. Behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål skal være underlagt fornødne garantier for registreredes rettigheder og frihedsrettigheder i overensstemmelse med denne forordning. 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 disse formål 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.

2. Når personoplysninger behandles til 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.

3. Når personoplysninger behandles til arkivformål i samfundets interesse, kan EU-retten eller medlemsstaternes nationale ret fastsætte undtagelser fra de rettigheder, der er omhandlet i artikel 15, 16, 18, 19, 20 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.

4. Når behandling som omhandlet i stk. 2 og 3 samtidig tjener et andet formål, anvendes undtagelser kun på behandling til de formål, der er omhandlet i nævnte stykker.

Artikel 90

Tavshedspligt

1. Medlemsstaterne kan vedtage specifikke regler om tilsynsmyndighedernes beføjelser i henhold til artikel 58, stk. 1, litra e) og f), vedrørende dataansvarlige eller databehandlere, der i henhold til EU-ret eller medlemsstaternes nationale ret eller regler fastsat af nationale kompetente organer er underlagt faglig eller anden tilsvarende tavshedspligt, hvis dette er nødvendigt og rimeligt for at forene retten til beskyttelse af personoplysninger med tavshedspligt. Disse regler gælder kun for personoplysninger, som den dataansvarlige eller databehandleren har modtaget som et resultat af eller indhentet under en aktivitet, der er underlagt denne tavshedspligt.

2. Hver medlemsstat giver senest den 25. maj 2018 Kommissionen meddelelse om de regler, som den vedtager i henhold til stk. 1, og underretter den straks om alle senere ændringer, der berører dem.

Artikel 91

Kirkers og religiøse sammenslutningers eksisterende databeskyttelsesregler

1. Hvis kirker og religiøse sammenslutninger eller samfund i en medlemsstat på tidspunktet for denne forordnings ikrafttræden anvender omfattende regler om beskyttelse af fysiske personer hvad angår behandling, kan disse eksisterende regler fortsat finde anvendelse, forudsat at de bringes i overensstemmelse med denne forordning.

2. Kirker og religiøse sammenslutninger, der anvender omfattende regler i henhold til denne artikels stk. 1, underlægges tilsyn af en uafhængig tilsynsmyndighed, som kan være specifik, forudsat at den opfylder betingelserne i kapitel VI.

KAPITEL X

Delegerede retsakter og gennemførelsesforanstaltninger

Artikel 92

Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 12, stk. 8, og artikel 43, stk. 8, tillægges Kommissionen for en ubegrænset periode fra den 24.maj 2016.

3. Den i artikel 12, stk. 8, og artikel 43, stk. 8, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

5. En delegeret retsakt vedtaget i henhold til artikel 12, stk. 8, og artikel 43, stk. 8, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på tre måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet eller Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med tre måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 93

Udvalgsprocedure

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

3. Når der henvises til dette stykke, finder artikel 8 i forordning (EU) nr. 182/2011 sammenholdt med dennes artikel 5 anvendelse.

KAPITEL XI

Afsluttende bestemmelser

Artikel 94

Ophævelse af direktiv 95/46/EF

1. Direktiv 95/46/EF ophæves med virkning fra den 25. maj 2018.

2. Henvisninger til det ophævede direktiv gælder som henvisninger til denne forordning. Henvisninger til Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved artikel 29 i direktiv 95/46/EF, gælder som henvisninger til Det Europæiske Databeskyttelsesråd oprettet ved denne forordning.

Artikel 95

Forhold til direktiv 2002/58/EF

Denne forordning indfører ikke yderligere forpligtelser for fysiske eller juridiske personer for så vidt angår behandling i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet i Unionen for så vidt angår spørgsmål, hvor de er underlagt specifikke forpligtelser med samme formål som det, der er fastsat i direktiv 2002/58/EF.

Artikel 96

Forhold til tidligere indgåede aftaler

Internationale aftaler, der omfatter overførsel af personoplysninger til tredjelande eller internationale organisationer, som er indgået af medlemsstaterne inden den 24. maj 2016, og som overholder den EU-ret, der finder anvendelse inden denne dato, forbliver i kraft, indtil de ændres, erstattes eller ophæves.

Artikel 97

Kommissionsrapporter

1. Senest den 25. maj 2020 og hvert fjerde år derefter forelægger Kommissionen Europa-Parlamentet og Rådet en rapport om evaluering og revision af denne forordning.

2. I forbindelse med de i stk. 1 omhandlede evalueringer og revisioner undersøger Kommissionen navnlig, hvordan følgende anvendes og fungerer:

a) kapitel V om overførsel af personoplysninger til tredjelande eller internationale organisationer, særlig med hensyn til afgørelser vedtaget i henhold til denne forordnings artikel 45, stk. 3, og afgørelser vedtaget på grundlag af artikel 25, stk. 6, i direktiv 95/46/EF

b) kapitel VII om samarbejde og sammenhæng.

3. Kommissionen kan med henblik på stk. 1 anmode om oplysninger fra medlemsstaterne og tilsynsmyndighederne.

4. Når Kommissionen foretager evaluering og revision, jf. stk. 1 og 2, tager den hensyn til holdninger og resultater fra Europa-Parlamentet, fra Rådet og fra andre relevante organer eller kilder.

5. Kommissionen forelægger om nødvendigt relevante forslag til ændring af denne forordning, navnlig under hensyntagen til udviklingen inden for informationsteknologi og i lyset af fremskridtene i informationssamfundet.

Artikel 98

Gennemgang af andre EU-retsakter om databeskyttelse

Hvis det er relevant, fremsætter Kommissionen lovgivningsforslag til ændring af andre EU-retsakter om beskyttelse af personoplysninger for at sikre ensartet og konsekvent beskyttelse af fysiske personer i forbindelse med behandling. Dette gælder især bestemmelser om beskyttelse af fysiske personer i forbindelse med EU-institutioners, -organers, -kontorers og -agenturers behandling og om fri udveksling af sådanne oplysninger.

Artikel 99

Ikrafttræden og anvendelse

1. Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

2. Den anvendes fra den 25. maj 2018.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 27. april 2016.

På Europa-Parlamentets vegne	*På Rådets vegne*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
Formand	*Formand*