



Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)¹

Afsnit I

Indledende bestemmelser

Kapitel 1

Lovens materielle anvendelsesområde

§ 1. Loven supplerer og gennemfører Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, jf. bilag til denne lov.

Stk. 2. Loven og databeskyttelsesforordningen gælder for al behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register. Loven og databeskyttelsesforordningen gælder dog ikke i det omfang, der er nævnt i databeskyttelsesforordningen artikel 2, stk. 2, litra b-d.

¹ Som bilag til loven er medtaget Europa-Parlamentets og Rådets forordning nr. 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), EU-Tidende 2016, nr. L 119, side 1. Ifølge artikel 288 i EUF-traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af forordningen i lovens bilag er således udelukkende begrundet i praktiske hensyn og berører ikke forordningens umiddelbare gyldighed i Danmark.

Stk. 3. Regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, går forud for reglerne i denne lov.

Stk. 4. I denne lov forstås ved databeskyttelsesforordningen: Europa-Parlamentets og Rådets forordning nr. 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).

§ 2. Lovens § 8, § 10 og § 11, stk. 1, samt databeskyttelsesforordningens artikel 5, stk. 1-3, artikel 6, artikel 9 og artikel 10 gælder også for manuel videregivelse af personoplysninger til en anden forvaltningsmyndighed. Datatilsynet fører i overensstemmelse med lovens kapitel 10 tilsyn med videregivelse som nævnt i 1. pkt.

Stk. 2. Loven og databeskyttelsesforordningen gælder endvidere for behandling af oplysninger om virksomheder mv., hvis denne behandling udføres for kreditoplysningsbureauer. Tilsvarende gælder for så vidt angår behandlinger, som er omfattet af § 26, stk. 1, nr. 1.

Stk. 3. Kapitel 4 gælder også for behandling af oplysninger om virksomheder m.v., jf. § 1, stk. 1.

Stk. 4. Loven og databeskyttelsesforordningen gælder for enhver form for behandling af personoplysninger i forbindelse med tv-overvågning.

Stk. 5. Loven og databeskyttelsesforordningen finder anvendelse på afdøde personer i 10 år efter vedkommendes død.

Stk. 6. Justitsministeren kan efter forhandling med vedkommende minister fastsætte regler om, at loven og databeskyttelsesforordningen skal finde anvendelse på afdøde personer i en længere eller kortere periode end angivet i stk. 5.

Stk. 7. Uden for de tilfælde, der er nævnt i stk. 2, kan justitsministeren fastsætte regler om, at lovens regler helt eller delvis skal finde anvendelse på behandling af oplysninger om virksomheder m.v., som udføres for private.

Stk. 8. Uden for de tilfælde, der er nævnt i stk. 3, kan vedkommende minister fastsætte regler om, at lovens regler helt eller delvis skal finde anven-

delse på behandling af oplysninger om virksomheder m.v., som udføres for den offentlige forvaltning.

§ 3. Loven og databeskyttelsesforordningens kapitel II-VII finder ikke anvendelse, hvis det vil være i strid med artikel 10 i Den Europæiske Menneskerettighedskonvention og artikel 11 i Den Europæiske Unions charter om grundlæggende rettigheder.

Stk. 2. Loven og databeskyttelsesforordningen finder ikke anvendelse på den behandling af personoplysninger, som udføres for eller af politiets og forswarets efterretningstjenester.

Stk. 3. Loven og databeskyttelsesforordningen finder ikke anvendelse på behandling af oplysninger, der foretages som led i Folketingets parlamentariske arbejde.

Stk. 4. Loven og databeskyttelsesforordningen finder ikke anvendelse på behandlinger, der er omfattet af lov om massemediers informationsdatabaser.

Stk. 5. Loven og databeskyttelsesforordningens kapitel II-VII og kapitel IX finder ikke 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. Dog gælder bestemmelserne i databeskyttelsesforordningens artikel 28 og 32.

Stk. 6. Loven og databeskyttelsesforordningens kapitel II-VII og kapitel IX gælder ikke for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte tekster, billeder og lydprogrammer, der omfattes af medieansvarslovens § 1, nr. 3, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen. Dog gælder bestemmelserne i databeskyttelsesforordningens artikel 28 og 32.

Stk. 7. Loven og databeskyttelsesforordningens kapitel II-VII og kapitel IX finder ikke anvendelse på manuelle arkiver over udklip fra offentliggjorte, trykte artikler, som udelukkende behandles i journalistisk øjemed. Dog gælder bestemmelserne i databeskyttelsesforordningens artikel 28 og 32.

Stk. 8. For behandling af oplysninger, som i øvrigt udelukkende finder sted i journalistisk øjemed, gælder alene bestemmelserne i databeskyttelsesforordningens artikel 28 og 32. Det samme gælder for behandling af oplysninger, som udelukkende sker med henblik på kunstnerisk eller litterær virksomhed.

Stk. 9. Justitsministeren kan efter forhandling med vedkommende minister fastsætte regler om, at personoplysninger, der behandles i nærmere bestemte IT-systemer, og som føres af eller for den offentlige forvaltning, alene må opbevares her i landet.

Stk. 10. Forsvarsministeren kan fastsætte regler om, at loven og databeskyttelsesforordningen helt eller delvist ikke finder anvendelse på Forsvarets behandling af personoplysninger i forbindelse med Forsvarets internationale operative virke.

Kapitel 2

Lovens geografiske område

§ 4. Loven og regler udstedt i medfør af loven gælder for behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i Danmark, uanset om behandlingen finder sted i EU.

Stk. 2. Loven og regler udstedt i medfør af loven gælder endvidere for den behandling, som udføres for danske diplomatiske repræsentationer.

Stk. 3. Loven og regler udstedt i medfør af loven gælder for behandling af personoplysninger om registrerede, der befinder sig i Danmark, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i EU, hvis behandlingsaktiviteterne vedrører:

- a) udbud af varer eller tjenester til sådanne registrerede, der befinder sig i Danmark, uanset om betaling fra den registrerede er påkrævet, eller
- b) overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Danmark.

Afsnit II

Behandlingsregler

Kapitel 3

Behandling af oplysninger

§ 5. Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål.

Stk. 2. For at afgøre, om behandling til et andet formål er forenelig med det formål, som personoplysningerne oprindeligt blev indsamlet til, jf. stk. 1, tager den dataansvarlige efter databeskyttelsesforordningens artikel 6, stk. 4, bl.a. hensyn til følgende:

- 1) enhver forbindelse mellem det formål, som personoplysningerne er indsamlet til, og formålet med den påtænkte viderebehandling,
- 2) den sammenhæng, hvori personoplysningerne er blevet indsamlet, navnlig med hensyn til forholdet mellem den registrerede og den dataansvarlige,
- 3) personoplysningernes art, navnlig om særlige kategorier af personoplysninger behandles, jf. artikel 9, eller om personoplysninger vedrørende straffedomme og lovovertrædelser behandles, jf. artikel 10,
- 4) den påtænkte viderebehandlings mulige konsekvenser for de registrerede, og
- 5) tilstedeværelse af fornødne garantier, som kan omfatte kryptering eller pseudonymisering.

Stk. 3. Uanset stk. 1-2 kan vedkommende minister efter forhandling med justitsministeren og inden for rammerne af databeskyttelsesforordningens artikel 23 fastsætte nærmere regler om, at personoplysninger af offentlige myndigheder må viderebehandles til andre formål, end de oprindeligt var indsamlet til, uafhængigt af formålenes forenelighed. 1. pkt. finder ikke anvendelse på § 10.

§ 6. Behandling af personoplysninger må finde sted, hvis mindst en af betingelserne i databeskyttelsesforordningens artikel 6, stk. 1, litra a-f, er opfyldt.

Stk. 2. Finder databeskyttelsesforordningens artikel 6, stk. 1, litra a, anvendelse i forbindelse med udbud af informationssamfundstjenester direkte til børn, er behandling af personoplysninger om et barn lovlig, hvis barnet er mindst 13 år.

Stk. 3. Er barnet under 13 år, er behandling kun lovlig, hvis og i det omfang samtykke gives eller godkendes af indehaveren af forældremyndigheden over barnet.

§ 7. Forbuddet mod behandling af følsomme personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, gælder ikke i tilfælde, hvor betingelserne for behandling af personoplysninger i databeskyttelsesforordningens artikel 9, stk. 2, litra a, c, d, e eller f, er opfyldt.

Stk. 2. Behandling af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, kan ske, hvis behandling er nødvendig for at overholde den dataansvarliges eller den registreredes arbejdsretlige forpligtelser og specifikke rettigheder, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra b.

Stk. 3. Behandling af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, kan ske, hvis behandling af oplysninger er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt jf. databeskyttelsesforordningens artikel 9, stk. 2, litra h.

Stk. 4. Behandling af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, kan ske hvis behandling af oplysninger er nødvendig af hensyn til væsentlige samfundsinteresse, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra g. Tilsynsmyndigheden giver tilladelse hertil, hvis behandlingen efter 1. pkt. ikke foretages af eller for en offentlig myndighed. Der kan i en tilladelse efter 2. pkt. fastsættes nærmere vilkår for behandlingen.

Stk. 5. Udenfor de i stk. 1-4 nævnte tilfælde kan vedkommende minister efter forhandling med justitsministeren og inden for databeskyttelsesforordningens rammer fastsætte nærmere regler om behandling af personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1.

§ 8. For den offentlige forvaltning må der ikke behandles oplysninger om strafbare forhold, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver.

Stk. 2. De oplysninger, der er nævnt i stk. 1, må ikke videregives. Videregivelse kan dog ske, hvis

- 1) den registrerede har givet sit udtrykkelige samtykke til videregivelsen,
- 2) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrundes hemmeligholdelse, herunder hensynet til den, oplysningen angår,
- 3) videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe, eller
- 4) videregivelsen er nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige.

Stk. 3. Private må behandle oplysninger om strafbare forhold, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Herudover kan behandling ske, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede.

Stk. 4. De oplysninger, der er nævnt i stk. 3, må ikke videregives uden den registreredes udtrykkelige samtykke. Videregivelse kan dog ske uden samtykke, når det sker til varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrundes hemmeligholdelse.

Stk. 5. Behandling af oplysninger i de tilfælde, der er reguleret i stk. 1-4, kan i øvrigt finde sted, hvis betingelserne i § 7 er opfyldt.

§ 9. Oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, og 10 må behandles, hvis dette alene sker med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for førelsen af systemerne.

Stk. 2. De af stk. 1 omfattede oplysninger må ikke senere behandles i andet øjemed. Det samme gælder behandling af andre oplysninger, som alene foretages med henblik på at føre retsinformationssystemer, jf. forordningens artikel 6.

Stk. 3. Tilsynsmyndigheden kan meddele nærmere vilkår for behandlinger, der er nævnt i stk. 1. Tilsvarende gælder for de oplysninger, der er nævnt i forordningens artikel 6, og som alene behandles i forbindelse med førelsen af retsinformationssystemer.

§ 10. Oplysninger som nævnt i databeskyttelsesforordningens artikel 9, stk. 1, og artikel 10 må behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig af hensyn til udførelsen af undersøgelserne.

Stk. 2. De oplysninger, der er omfattet af stk. 1, må ikke senere behandles i andet end videnskabeligt eller statistisk øjemed. Det samme gælder behandling af andre oplysninger, som alene foretages i statistisk eller videnskabeligt øjemed, jf. databeskyttelsesforordningens artikel 6.

Stk. 3. Oplysninger omfattet af stk. 1 og 2 må kun videregives til tredje- mand efter forudgående tilladelse fra tilsynsmyndigheden. Tilsynsmyndig- heden kan stille nærmere vilkår for videregivelsen.

Stk. 4. Sundhedsministeren kan efter forhandling med justitsministeren uanset stk. 2 fastsætte regler om, at oplysninger som nævnt i databeskyttel- sesforordningens artikel 6 og 9, som er behandlet med henblik på at udføre sundhedsvidenskabelig forskning, senere kan behandles i andet end stati- stisk eller videnskabeligt øjemed, hvis behandlingen er nødvendig af hen- syn til varetagelse af den registreredes vitale interesser.

§ 11. Offentlige myndigheder kan behandle oplysninger om personnum- mer med henblik på en entydig identifikation eller som journalnummer.

Stk. 2. Private må behandle oplysninger om personnummer, når

- 1) det følger af lovgivningen,
- 2) den registrerede har givet samtykke hertil i overensstemmelse med data- beskyttelsesforordningens artikel 7,
- 3) behandlingen alene finder sted til videnskabelige eller statistiske formål, eller hvis der er tale om videregivelse af oplysninger om personnummer, når videregivelsen er et naturligt led i den normale drift af virksomheder m.v. af den pågældende art, og når videregivelsen er af afgørende betyd- ning for at sikre en entydig identifikation af den registrerede, eller videre- givelsen kræves af en offentlig myndighed, eller
- 4) betingelserne i § 7 er opfyldt.

Stk. 3. Uanset bestemmelsen i stk. 2, nr. 3, må personnummer ikke offent- liggøres, medmindre der er givet samtykke i overensstemmelse med data- beskyttelsesforordningens artikel 7.

§ 12. Behandling af personoplysninger i forbindelse med ansættelsesforhold omfattet af artikel 6, stk. 1, og artikel 9, stk. 1, i databeskyttelsesforordningen kan finde sted, hvis behandlingen er nødvendig for at overholde den dataansvarliges eller den registreredes arbejdsretlige forpligtelser eller rettigheder, som fastlagt i anden lovgivning eller kollektive overenskomster.

Stk. 2. Behandling af oplysninger som nævnt i stk. 1 må også finde sted, hvis behandlingen er nødvendig for, at den dataansvarlige kan forfølge en legitim interesse som udspringer af anden lovgivning eller kollektive overenskomster, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, går forud herfor.

Stk. 3. Behandling af personoplysninger i ansættelsesforhold kan finde sted på baggrund af den registreredes samtykke i overensstemmelse med artikel 7 i databeskyttelsesforordningen.

§ 13. En virksomhed må ikke videregive oplysninger om en forbruger til en anden virksomhed til brug ved markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed, medmindre forbrugeren har givet sit udtrykkelige samtykke hertil. Et samtykke skal indhentes i overensstemmelse med reglerne i markedsføringslovens § 10.

Stk. 2. Videregivelse og anvendelse som nævnt i stk. 1 kan dog ske uden samtykke, hvis der er tale om generelle kundeoplysninger, der danner grundlag for inddeling i kundekategorier, og hvis betingelserne i databeskyttelsesforordningens artikel 6, stk. 1, litra f, er opfyldt.

Stk. 3. Der kan efter stk. 2 ikke videregives eller anvendes oplysninger som nævnt i databeskyttelsesforordningens artikel 9, stk. 1, og denne lovs § 8, stk. 1. Justitsministeren kan fastsætte yderligere begrænsninger i adgangen til at videregive eller anvende bestemte typer af oplysninger efter stk. 2.

Stk. 4. Inden en virksomhed videregiver oplysninger om en forbruger til en anden virksomhed med henblik på direkte markedsføring eller anvender oplysningerne på vegne af en anden virksomhed i dette øjemed, skal den undersøge i CPR, om forbrugeren har frabedt sig henvendelser i markedsføringsøjemed.

Stk. 5. Dataansvarlige, der med henblik på markedsføring sælger fortegnelser over grupper af personer, eller som for tredjemand foretager adressering eller udsendelse af meddelelser til sådanne grupper, må kun behandle

- 1) oplysninger om navn, adresse, stilling, erhverv, e-postadresse, telefon- og telefaxnummer,
- 2) oplysninger, der indgår i erhvervsregistre, som i henhold til lov eller bestemmelser fastsat i henhold til lov er beregnet til at informere offentligheden, samt
- 3) andre oplysninger, hvis den registrerede har givet udtrykkeligt samtykke dertil. Et samtykke skal indhentes i overensstemmelse med markedsføringslovens § 10.

Stk. 6. Behandling af oplysninger som nævnt i stk. 4 må ikke omfatte oplysninger som nævnt i databeskyttelsesforordningens artikel 9, stk. 1, og denne lovs § 8, stk. 1. Justitsministeren kan fastsætte yderligere begrænsninger i adgangen til at behandle bestemte typer af oplysninger.

§ 14. Oplysninger, der er omfattet af denne lov, kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Kapitel 4

Videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige

§ 15. Oplysninger om gæld til det offentlige kan efter bestemmelserne i dette kapitel videregives til kreditoplysningsbureauer.

Stk. 2. Oplysninger som nævnt i databeskyttelsesforordningens artikel 9, stk. 1, eller artikel 10 må ikke videregives til kreditoplysningsbureauer.

Stk. 3. Fortrolige oplysninger, som videregives efter reglerne i dette kapitel, anses ikke som følge af videregivelsen som offentligt tilgængelige.

§ 16. Oplysninger om gæld til det offentlige kan videregives til et kreditoplysningsbureau, hvis

- 1) det følger af lov eller bestemmelser fastsat i henhold til lov, eller
- 2) den samlede gæld er forfalden og overstiger 7.500 kr., idet der dog ikke heri må indgå gældsposter, der er omfattet af en overholdt aftale om henstand eller afdragsvis betaling.

Stk. 2. Det er en betingelse for videregivelse efter stk. 1, nr. 2, at den samlede gæld administreres af samme inddrivelsesmyndighed.

Stk. 3. Det er endvidere en betingelse for videregivelse efter stk. 1, nr. 2, at

- 1) gælden kan inddrives ved udpantning, og der er fremsendt 2 rykkere til skyldneren,
- 2) der er foretaget eller forsøgt foretaget udlæg for kravet,
- 3) kravet er fastslået ved endelig dom, eller
- 4) det offentlige har erhvervet skyldnerens skriftlige erkendelse af den forfaldne gæld.

§ 17. Myndigheden skal give skyldneren skriftlig meddelelse herom, forinden videregivelse finder sted. Videregivelse må tidligst ske 4 uger efter, at denne meddelelse er givet.

Stk. 2. Den i stk. 1 nævnte meddelelse skal indeholde oplysninger om,

- 1) hvilke oplysninger der vil blive videregivet,
- 2) til hvilket kreditoplysningsbureau videregivelsen vil ske,
- 3) hvornår videregivelse vil finde sted, og
- 4) at videregivelse ikke vil ske, hvis betaling af gælden sker inden videregivelsen, eller der indrømmes henstand eller indgås og overholdes en aftale om afdragsvis betaling.

§ 18. Vedkommende minister kan fastsætte nærmere regler om fremgangsmåden ved videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige. Der kan i den forbindelse fastsættes regler om, at oplysninger om visse former for gæld til det offentlige ikke må videregives eller kun må videregives, hvis yderligere betingelser end de i § 16 nævnte er opfyldt.

Kapitel 5

Kreditoplysningsbureauer

§ 19. Den, som ønsker at drive virksomhed med behandling af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse (kreditoplysningsbureau), skal indhente tilladelse hertil fra Datatilsynet, inden behandlingen påbegyndes, jf. § 26, stk. 1, nr. 2.

§ 20. Kreditoplysningsbureauer må kun behandle oplysninger, som efter deres art er af betydning for bedømmelse af økonomisk soliditet og kreditværdighed.

Stk. 2. Kreditoplysningsbureauer må ikke behandle oplysninger som nævnt i databeskyttelsesforordningens artikel 9, stk. 1, eller artikel 10.

Stk. 3. Oplysninger om forhold, der taler imod kreditværdighed, og som er mere end 5 år gamle, må ikke behandles, medmindre det i det enkelte tilfælde er åbenbart, at forholdet er af afgørende betydning for bedømmelsen af den pågældendes økonomiske soliditet og kreditværdighed.

Stk. 4. Databeskyttelsesforordningens artikel 12-19 gælder for behandling af oplysninger om virksomheder m.v., hvis denne behandling udføres for kreditoplysningsbureauer.

§ 21. Oplysninger om økonomisk soliditet og kreditværdighed til abonnenter må kun meddeles skriftligt. Kreditoplysningsbureauet kan dog meddele summariske oplysninger mundtligt eller på lignende måde, såfremt spørgerens navn og adresse noteres og opbevares i mindst 6 måneder.

Stk. 2. Kreditoplysningsbureauers publikationer må kun indeholde oplysninger i summarisk form og kun udsendes til personer eller virksomheder, der abonnerer på meddelelser fra bureauet. Publikationerne må ikke indeholde oplysninger om de registreredes personnummer.

Stk. 3. Summariske oplysninger om skyldforhold må kun videregives, hvis oplysningerne hidrører fra Statstidende, er indberettet af en offentlig myndighed efter reglerne i kapitel 4, eller hvis oplysningerne vedrører skyldforhold til samme kreditor på mere end 1.000 kr., og kreditor enten har erhvervet den registreredes skriftlige erkendelse af en forfalden gæld, eller hvis der er foretaget retslige skridt mod den pågældende. Oplysninger om endelig godkendt gældssanering må dog ikke videregives. De regler, der er nævnt i 1. og 2. pkt. gælder tillige for videregivelse af summariske oplysninger om skyldforhold i forbindelse med udarbejdelse af bredere kreditbedømmelser.

Stk. 4. Videregivelse af summariske oplysninger om enkeltpersoners skyldforhold må kun ske på en sådan måde, at oplysningerne ikke kan danne grundlag for vurderingen af økonomisk soliditet og kreditværdighed for andre end de pågældende enkeltpersoner.

Afsnit III

Registreredes rettigheder

Kapitel 6

Begrænsninger i registreredes rettigheder

§ 22. Bestemmelserne i databeskyttelsesforordningens artikel 13, stk. 1-3, artikel 14, stk. 1-4, og artikel 15 gælder ikke, hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv.

Stk. 2. Undtagelse fra bestemmelserne i databeskyttelsesforordningens artikel 12-15, kan tillige gøres, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige interesser, herunder navnlig til

- 1) statens sikkerhed,
- 2) forsvaret,
- 3) den offentlige sikkerhed,
- 4) forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed,
- 5) 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,
- 6) beskyttelse af retsvæsenets uafhængighed og retssager,
- 7) forebyggelse, efterforskning, afsløring og retsforfølgning i forbindelse med brud på etiske regler for lovregulerede erhverv,
- 8) kontrol-, tilsyns- eller reguleringsfunktioner, herunder opgaver af midlertidig karakter, der er forbundet med offentlig myndighedsudøvelse i de tilfælde, der er omhandlet i nr. 1-5 og 7,
- 9) beskyttelse af den registrerede eller andres rettigheder og frihedsrettigheder, og
- 10) håndhævelse af civilretlige krav.

Stk. 3. Oplysninger, der behandles for den offentlige forvaltning som led i administrativ sagsbehandling, kan undtages fra retten til indsigt efter data-

beskyttelsesforordningens artikel 15, stk. 1, i samme omfang som efter reglerne i §§ 19-29 og 35 i lov om offentlighed i forvaltningen.

Stk. 4. Der er ikke ret til indsigt efter i databeskyttelsesforordningens artikel 15, stk. 1, i oplysninger, der behandles for domstolene, hvis oplysningerne indgår i tekst, som ikke foreligger i endelig form. Dette gælder dog ikke, hvis oplysningerne er videregivet til en tredjemand. Der er ikke ret til indsigt i voteringsprotokoller og andre referater af domstolenes rådslagning samt materiale udarbejdet af domstolene til brug for rådslagningen.

Stk. 5. Databeskyttelsesforordningens artikel 15, stk. 1, finder ikke anvendelse, hvis oplysningerne udelukkende behandles i videnskabeligt øjemed, eller hvis oplysningerne kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker.

§ 23. Oplysningspligten efter databeskyttelsesforordningens artikel 13, stk. 3, og artikel 14, stk. 4, finder ikke anvendelse, når offentlige myndigheder viderebehandler personoplysningerne til et andet formål end det, hvortil de er indsamlet og viderebehandlingen sker på baggrund af regler fastsat efter lovens § 5, stk. 3.

Afsnit IV

Supplerende bestemmelser til databeskyttelsesforordningens kapitel IV

Kapitel 7

Tavshedspligt for databeskyttelsesrådgivere

§ 24. Databeskyttelsesrådgivere, der er udpeget efter databeskyttelsesforordningens artikel 37, stk. 1, litra b og c, må ikke uberettiget videregive eller udnytte oplysninger, som de under udøvelsen af deres hverv som databeskyttelsesrådgiver er blevet bekendt med.

Kapitel 8

Akkreditering af certificeringsorganer

§ 25. Datatilsynet er bemyndiget til at akkreditere certificeringsorganer, jf. databeskyttelsesforordningens artikel 43, stk. 1, litra a.

Afsnit V

Tilladelse til behandling

Kapitel 9

Tilladelse til behandlinger, der foretages for en privat dataansvarlig

§ 26. Forinden iværksættelse af en behandling skal Datatilsynets tilladelse indhentes, når

- 1) behandlingen af oplysningerne sker med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret,
- 2) behandlingen sker med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed, eller
- 3) behandlingen udelukkende finder sted med henblik på at føre retsinformationssystemer.

Stk. 2. Justitsministeren kan fastsætte regler om undtagelser fra bestemmelserne i stk. 1.

Stk. 3. Justitsministeren kan fastsætte regler om, at der forinden iværksættelse af andre behandlinger end dem, der er nævnt i stk. 1, skal indhentes tilladelse fra tilsynet.

Stk. 4. Tilsynet kan i forbindelse med meddelelse af tilladelse efter stk. 1 eller 3 fastsætte vilkår for udførelsen af behandlingerne til beskyttelse af de registreredes privatliv.

Stk. 5. Forinden iværksættelse af ændringer i de behandlinger, der er nævnt i stk. 1 eller 3, skal Datatilsynets tilladelse indhentes på ny, hvis der er tale om væsentlige ændringer.

Afsnit VI

Uafhængige tilsynsmyndigheder

Kapitel 10

Datatilsynet

§ 27. Datatilsynet, der består af et råd og et sekretariat, fører i overensstemmelse med databeskyttelsesforordningens kapitel VI tilsyn med enhver behandling, der omfattes af denne lov, databeskyttelsesforordningen og anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, jf. dog lovens kapitel 11.

Stk. 2. Tilsynets daglige forretninger varetages af et sekretariat, der ledes af en direktør.

Stk. 3. Justitsministeren nedsætter Datarådet, som består af en formand, der er dommer, og af 7 andre medlemmer. Erhvervsministeren og ministeren for offentlig innovation udnævner hver ét de 7 andre medlemmer omfattet af 1. pkt. Justitsministeren kan udpege stedfortrædere for medlemmerne. Formanden, medlemmerne og stedfortræderne for disse udpeges for 4 år. Der kan ske genudpegning to gange. Udpegelsen af formand, medlemmer og stedfortrædere for disse sker på baggrund af disses faglige kvalifikationer.

Stk. 4. Rådet fastsætter sin forretningsorden og de nærmere regler om arbejdsfordeling mellem råd og sekretariat.

Stk. 5. Udpegelsen af formand, medlemmer og stedfortrædere for disse er betinget af, at de pågældende sikkerhedsgodkendes, og at godkendelsen opretholdes i hele embedsperioden.

Stk. 6. Hvervet som formand, medlem eller stedfortræder ophører ved udgangen af embedsperioden eller ved frivillig fratræden.

Stk. 7. Formanden, medlemmer og stedfortrædere for disse kan alene afskediges i tilfælde af alvorligt embedsmisbrug, eller hvis disse ikke længere opfylder betingelserne for at varetage hvervet.

Stk. 8. Sekretariatets personale samt Datarådets formand, medlemmer og stedfortrædere for disse kan kun have bibeskæftigelse, for så vidt og i det omfang det er foreneligt med udøvelsen af de pligter, der er knyttet til stillingen eller hvervet.

Stk. 9. Datatilsynet repræsenterer tilsynsmyndighederne i Det Europæiske Databeskyttelsesråd.

§ 28. Ved udarbejdelse af lovforslag, bekendtgørelser, cirkulærer eller lignende generelle retsfor skrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger, skal der indhentes en udtalelse fra Datatilsynet.

§ 29. Datatilsynet kan kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under databeskyttelsesforordningens og lovens bestemmelser.

Stk. 2. Datatilsynets medlemmer og personale har mod behørig legitimation til enhver tid uden retskendelse adgang til alle lokaler, hvorfra en behandling af personoplysninger foretages.

§ 30. Datatilsynets afgørelser efter denne lov kan ikke indbringes for anden administrativ myndighed.

Stk. 2. Datatilsynet kan indbringe spørgsmål om overtrædelser af denne lov for retten i den borgerlige retsplejes former.

§ 31. Hvis der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet efter artikel 45 i databeskyttelsesforordningen, kan Datatilsynet i særlige tilfælde forbyde, begrænse eller suspendere overførsel af særlige kategorier af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, til et tredjeland eller en international organisation.

§ 32. Datatilsynet kan videregive oplysninger til tilsynsmyndigheder i andre medlemsstater i det omfang, det er nødvendigt for at påse overholdelsen af bestemmelserne i denne lov, databeskyttelsesforordningen eller den pågældende medlemsstats databeskyttelseslovgivning.

§ 33. Datatilsynet kan offentliggøre sine udtalelser og afgørelser. Bestemmelsen i § 22 finder også anvendelse.

§ 34. Datatilsynet og Domstolsstyrelsen samarbejder, i det omfang det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle relevante oplysninger.

§ 35. Justitsministeren kan fastsætte nærmere regler om, at Datatilsynet og Domstolsstyrelsen har yderligere beføjelser end dem, der er omhandlet i databeskyttelsesforordningens artikel 58, stk. 1, 2 og 3.

§ 36. Datatilsynet kan bestemme, at ansøgninger om tilladelse efter denne lov og ændringer heri kan eller skal indgives på nærmere angiven måde.

Stk. 2. Justitsministeren kan fastsætte regler om betaling af gebyr for indgivelse af ansøgninger om tilladelser i henhold til denne lov, herunder regler om gebyrets størrelse og om, at en tilladelse ikke meddeles, før betaling er sket.

Stk. 3. Justitsministeren kan fastsætte regler om betaling af gebyr efter databeskyttelsesforordningens artikel 57, stk. 4.

Kapitel 11

Tilsyn med domstolene

§ 37. Domstolsstyrelsen fører i overensstemmelse med databeskyttelsesforordningens kapitel VI tilsyn med behandling af oplysninger, der foretages for domstolene, når disse ikke handler i deres egenskab af domstol.

Stk. 2. For anden behandling af oplysninger træffes afgørelse af vedkommende ret. Afgørelsen kan kæres til højere ret. For særlige domstole, hvis afgørelser ikke kan indbringes for højere ret, kan den afgørelse, der er nævnt i 1. pkt., kæres til den landsret, i hvis kreds retten er beliggende. Kærefristen er 4 uger fra den dag, afgørelsen er meddelt den pågældende.

§ 38. For Domstolsstyrelsens udøvelse af tilsyn i henhold til § 37 gælder bestemmelserne i §§ 29 og 34. Domstolsstyrelsens afgørelser er endelige.

Afsnit VII

Retsmidler, ansvar og sanktioner

Kapitel 12

Retsmidler, ansvar og sanktioner

§ 39. Den registrerede eller dennes repræsentant kan klage til vedkommende tilsynsmyndighed over behandling af oplysninger vedrørende den registrerede, jf. databeskyttelsesforordningens artikel 77.

Stk. 2. Tilsynsmyndighedernes afgørelser, undladelser af at behandle en klage fra en registreret eller manglende underretning kan af den registrerede eller dennes repræsentant indbringes for domstolene i den borgerlige retsplejes former, jf. databeskyttelsesforordningens artikel 78.

Stk. 3. Den registrerede eller dennes repræsentant kan indbringe spørgsmål om dataansvarliges og databehandlers overholdelse af denne lov for domstolene i den borgerlige retsplejes former, jf. databeskyttelsesforordningens artikel 79.

§ 40. Enhver person, som har lidt materiel eller immateriel skade som følge af en ulovlig behandlingsaktivitet eller enhver anden behandling i strid med denne lov og databeskyttelsesforordningen, har ret til erstatning efter databeskyttelsesforordningens artikel 82.

§ 41. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 6 måneder overtrædelse af:

- 1) den dataansvarliges og databehandlerens forpligtelser i henhold til databeskyttelsesforordningens artikel 8, 11, 25-39 og 42 og 43
- 2) certificeringsorganets forpligtelser i henhold til databeskyttelsesforordningens artikel 42 og 43
- 3) kontrolorganets forpligtelser i henhold til databeskyttelsesforordningens artikel 41, stk. 4.

Stk. 2. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 6 måneder overtrædelse af:

- 1) de grundlæggende principper for behandling, herunder betingelserne for samtykke, i databeskyttelsesforordningens artikel 5, 6, 7, 9 og 10
- 2) de registreredes rettigheder i henhold til databeskyttelsesforordningens artikel 12-22
- 3) databeskyttelsesforordningens artikel 44-49 om overførsel af personoplysninger til en modtager i et tredjeland eller en international organisation

4) denne lovs §§ 9-13 og §§ 20-21

5) et påbud eller en midlertidig eller definitiv begrænsning af behandling eller tilsynsmyndighedens suspension af overførsel af oplysninger i henhold til databeskyttelsesforordningens artikel 58, stk. 2, eller manglende adgang i strid med artikel 58, stk. 1.

Stk. 3. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 6 måneder den dataansvarlige eller databehandler, der gør sig skyldig i manglende overholdelse af et påbud fra tilsynsmyndigheden som omhandlet i databeskyttelsesforordningens artikel 58, stk. 2.

Stk. 4. Databeskyttelsesforordningens artikel 83, stk. 2, skal følges ved pålægges af straf efter stk. 1-3.

Stk. 5. [stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder udestår]

Stk. 6. Databeskyttelsesrådgivere, der overtræder tavshedspligten i § 24, jf. databeskyttelsesforordningens artikel 38, stk. 5, straffes med bøde, medmindre strengere straf er forskyldt efter den øvrige lovgivning.

Stk. 7. I regler, der udstedes i medfør af loven, kan der fastsættes straf af bøde eller fængsel indtil 6 måneder.

Stk. 8. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

§ 42. Skønnes en overtrædelse af denne lov eller databeskyttelsesforordningen ikke at ville medføre højere straf end bøde, kan Datatilsynet tilkendegive, at sagen kan afgøres uden retslig forfølgning, hvis den, der har begået overtrædelsen, erklærer sig skyldig i overtrædelsen og erklærer sig rede til inden en nærmere angivet frist, der efter begæring kan forlænges, at betale en i tilkendegivelsen angivet bøde.

Stk. 2. Retsplejelovens regler om krav til indholdet af et anklageskrift og om, at en sigtet ikke er forpligtet til at udtale sig finder tilsvarende anvendelse på bødeforelæg.

Stk. 3. Betales bøden i rette tid, bortfalder videre forfølgning.

§ 43. Den, der driver eller er beskæftiget med virksomhed som nævnt i § 26 eller som privat databehandler opbevarer personoplysninger, kan ved dom for strafbart forhold frakendes retten hertil, såfremt det udviste forhold begrundes en nærliggende fare for misbrug. I øvrigt finder straffelovens § 79, stk. 3 og 4, anvendelse.

Kapitel 13

Afsluttende bestemmelser

§ 44. Vedkommende minister kan i særlige tilfælde og inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger efter forhandling med justitsministeren fastsætte nærmere regler for behandlinger, som udføres for den offentlige forvaltning.

Stk. 2. Justitsministeren kan inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger fastsætte nærmere regler for bestemte typer af behandlinger, som udføres for private dataansvarlige, herunder at bestemte typer oplysninger ikke må behandles.

§ 45. Justitsministeren kan fastsætte regler, som er nødvendige for at gennemføre de af Den Europæiske Unions udstedte beslutninger, som træffes med henblik på gennemførelse af databeskyttelsesforordningen, eller regler, som er nødvendige for at anvende de af Den Europæiske Unions udstedte retsakter på forordningens område.

§ 46. Loven træder i kraft den 25. maj 2018.

Stk. 2. Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger, som senest ændret ved lov nr. 426 af 3. maj 2017, ophæves.

§ 47. For behandlinger, hvortil der inden lovens ikrafttræden er opnået tilladelse efter § 50, stk. 1, nr. nr. 2-3 og nr. 5, i lov nr. 429 af 31. maj 2000 om behandling af personoplysninger, som senest ændret ved lov nr. 426 af 3. maj 2017, skal der ikke efter lovens ikrafttræden indhentes en ny tilladelse efter denne lovs § 26, stk. 1, nr. 1-3.

§ 48. Loven gælder ikke for Færøerne, men kan ved kongelig anordning sættes helt eller delvist i kraft for rigsmyndighedernes behandling af oplys-

ninger med de ændringer, som de færøske forhold tilsiger. Loven gælder ikke for Grønland, men kan ved kongelig anordning sættes helt eller delvist i kraft for Grønland med de ændringer, som de grønlandske forhold tilsiger.

**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.

- (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 ni-

veauet 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 manøvremargin, 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 ret-

tigheder, 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 [\(5\)](#).

- (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 [\(6\)](#) 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 erhvervmæssig eller kommerciel aktivitet. Personlige 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 [\(7\)](#). 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 medlem-

sstaternes 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 ⁽⁸⁾, 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.
- (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 incitament 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 værdipapirmarkedene, 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 lejlighedsvis 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 [\(9\)](#), til den fysiske person; et nummer, symbol eller særligt mærke, der tildeles en fysisk person for entydigt at identificere den fysiske person til sundhedsformål; oplysninger, der hidrører fra prøver eller undersøgelser af en legemsdel eller legemlig substans, herunder fra genetiske data og biologiske prøver; og enhver oplysning om f.eks. en sygdom, et handicap, en sygdomsrisiko, en sygehistorie, en sundhedsfaglig behandling eller den registreredes fysiologiske eller biomedicinske tilstand uafhængigt af kilden hertil, f.eks. fra en læge eller anden sundhedsperson, et hospital, medicinsk udstyr eller in vitro-diagnostik.
- (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 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, finansielt 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. Personoplys-

ninger 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 ⁽¹⁰⁾ 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 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 registre-

ret 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 informationssystemes 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 oprindeligt 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 sundhedsydelse, 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 medlemssta-

ternes 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 [\(11\)](#), dvs. alle elementer vedrørende sundhed, nemlig helbredstilstand, herunder sygelighed og invaliditet, determinanter med en indvirkning på helbredstilstanden, behov for sundhedspleje, ressourcer tildelt sundhedsplejen, ydelse af og almen adgang til sundhedspleje, udgifter til og finansiering af sundhedspleje samt dødsårsager. Sådan behandling af helbredsoplysninger af hensyn til samfundsinteresser bør ikke medføre, at tredjemænd såsom arbejdsgivere eller forsikringsselskaber og pengeinstitutter behandler personoplysninger til andre formål.
- (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 unødigt forsinkelse og senest inden for en måned og begrunde det, hvis vedkommende ikke agter at imødekomme sådanne anmodninger.
- (60) Principperne om rimelig og gennemsigtig behandling kræver, at den registrerede informeres om behandlingsaktivitetens 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 regi-

strerede. 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 udø-

ve 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 tredjemandes 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 straffetlige 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 af-

hjælpe 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 im-

plementeringsomkostningerne 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 unødigt 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 unødigt yderligere forsinkelse.
- (86) Den dataansvarlige bør underrette den registrerede om et brud på persondatasikkerheden uden unødigt 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 unødigt 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 finansiell 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 industri-sektor 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 af 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 databehandlers 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 [\(12\)](#), 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 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 lejlig-hedsvis 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 reguleringsorga-ner. 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 inter-esse. 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 socialsik-ringsmyndigheder 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 an-ses for lovlig, hvis den registrerede er ude af stand til at give sit samtykke. I mangel af en afgørelse om tilstrækkeligheden af beskyt-telsesniveauet 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 Kom-missionen 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 væ-re 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 gentagel-

ser, 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 retsfølgende 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 tilsyns-

myndighed, 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 besluttet 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 annullationsøgsmål 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 databehandlerens 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 [\(13\)](#) 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 sanktio-

ner 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 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 fast-

sættes 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 ⁽¹⁴⁾ opretholder og griber på ingen måde ind i beskyttelsesniveauet for fysiske personer med hensyn til behandling af personoplysninger i henhold til EU-retten og 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 »lokaftaler«, 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 registreredes 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 så-

som 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 langtids-sammenhæng 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 bestem-

melser i Europa-Parlamentets og Rådets forordning (EU) nr. 536/2014 ⁽¹⁵⁾ 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 ⁽¹⁶⁾ 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 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 ekspertni-

veau. 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) Undersøgellesproceduren 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 ⁽¹⁷⁾.

(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 ⁽¹⁸⁾, 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 —

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, for-

midling 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 personop-

lysninger, 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 samslutninger, 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 ⁽¹⁹⁾

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«)
 - 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 samfun-

dets 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 oprindeligt 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 be-

holde, 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 unødigt 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 unødigt 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 unødigt forsinkelse, og den dataansvarlige har pligt til at slette personoplysninger uden unødigt 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 be-

- handlingen 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 foranstalt-

ninger 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 or-

ganisationer

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 straf-fedomme 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 unødigt 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 unødigt 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 unødigt yderligere forsinkelse.

5. Den dataansvarlige dokumenterer alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de truffede 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 unødigt 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 tjensteydelseskontrakt.

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. Databeskyttelsesrådgive-

ren 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 tilsgagn, 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 databehandlers 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 databehandlers 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 ⁽²⁰⁾ 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
- 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 registrede 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 finansiell 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 domstolens 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 offent-

- ligheden 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 sa-

gen. 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 unødigt 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 begrundet 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 med-

lemmer 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 enig i udkastet til afgørelse.

4. Tilsynsmyndigheder og Kommissionen sender uden unødigt 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 unødigt 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

Twistbilægelse 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 unødigt 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 unødigt 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 begrundet 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 begrundet 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 virksom-

hedsregler, 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 ⁽²¹⁾.

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 for-

bindelse 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.

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 om-

handlet 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

M. SCHULZ

Formand

På Rådets vegne

J.A. HENNIS-PLASSCHAERT

Formand

⁽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](#)).

⁽⁵⁾ 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](#)).

⁽⁶⁾ 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](#)).

⁽⁷⁾ 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).

⁽⁸⁾ 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](#)).

⁽⁹⁾ 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](#)).

⁽¹⁰⁾ Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår i forbrugeraftaler ([EFT L 95 af 21.4.1993, s. 29](#)).

⁽¹¹⁾ 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](#)).

⁽¹²⁾ 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](#)).

- (13) 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](#)).
- (14) 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](#)).
- (15) 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](#)).
- (16) 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](#)).
- (17) [EUT C 192 af 30.6.2012, s. 7](#).
- (18) 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](#)).
- (19) Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informations-samfundets tjenester ([EUT L 241 af 17.9.2015, s. 1](#)).
- (20) 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](#)).
- (21) 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](#)).

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

- 1.1. Baggrund og formål
- 1.2. Lovforslagets indhold i hovedtræk
- 1.3. Overordnet om den retlige ramme for lovforslaget i forhold til databeskyttelsesforordningen

2. Lovforslagets hovedpunkter

- 2.1. Lovens materielle anvendelsesområde
 - 2.1.1. Gældende ret
 - 2.1.2. Databeskyttelsesforordningen
 - 2.1.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.2. Lovens geografiske anvendelsesområde
 - 2.2.1. Gældende ret
 - 2.2.2. Databeskyttelsesforordningen
 - 2.2.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.3. Behandlingsregler
 - 2.3.1. Formålsbestemthed
 - 2.3.1.1. Gældende ret
 - 2.3.1.2. Databeskyttelsesforordningen
 - 2.3.1.3. Justitsministeriets overvejelser og lovforslagets udformning
 - 2.3.2. Behandling af almindelige oplysninger
 - 2.3.2.1. Gældende ret
 - 2.3.2.2. Databeskyttelsesforordningen
 - 2.3.2.3. Justitsministeriets overvejelser og lovforslagets udformning
 - 2.3.3. Behandling af følsomme oplysninger
 - 2.3.3.1. Gældende ret
 - 2.3.3.2. Databeskyttelsesforordningen
 - 2.3.3.3. Justitsministeriets overvejelser og lovforslagets udformning
 - 2.3.4. Behandling af oplysninger om strafbare forhold
 - 2.3.4.1. Gældende ret
 - 2.3.4.2. Databeskyttelsesforordningen

- 2.3.4.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.3.5. Behandling af oplysninger i forbindelse med retsinformationssystemer
 - 2.3.5.1. Gældende ret
 - 2.3.5.2. Databeskyttelsesforordningen
 - 2.3.5.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.3.6. Behandling af oplysninger i statistik eller videnskabeligt øjemed
 - 2.3.6.1. Gældende ret
 - 2.3.6.2. Databeskyttelsesforordningen
 - 2.3.6.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.3.7. Behandling af oplysninger om personnummer
 - 2.3.7.1. Gældende ret
 - 2.3.7.2. Databeskyttelsesforordningen
 - 2.3.7.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.3.8. Behandling af oplysninger i forbindelse med ansættelsesforhold
 - 2.3.8.1. Gældende ret
 - 2.3.8.2. Databeskyttelsesforordningen
 - 2.3.8.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.3.9. Behandling i forbindelse med markedsføring mv.
 - 2.3.9.1. Gældende ret
 - 2.3.9.2. Databeskyttelsesforordningen
 - 2.3.9.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.3.10. Overførsel til arkiv.
 - 2.3.10.1. Gældende ret
 - 2.3.10.2. Databeskyttelsesforordningen
 - 2.3.10.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.3.11. Kreditoplysningsområdet
 - 2.3.11.1. Gældende ret
 - 2.3.11.2. Databeskyttelsesforordningen
 - 2.3.11.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.4. Den registreredes rettigheder

- 2.4.1. Gældende ret
 - 2.4.2. Databeskyttelsesforordningen
 - 2.4.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.5. Supplerende bestemmelser til databeskyttelsesforordningens kapitel IV
 - 2.5.1. Gældende ret
 - 2.5.2. Databeskyttelsesforordningen
 - 2.5.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.6. Tilladelse til behandling
 - 2.6.1. Gældende ret
 - 2.6.2. Databeskyttelsesforordningen
 - 2.6.3. Justitsministeriets overvejelser og lovforslagets udformning
- 2.7. Tilsyn
 - 2.7.1. Gældende ret
 - 2.7.2. Databeskyttelsesforordningen
 - 2.7.3. Justitsministeriet overvejelser og lovforslagets udformning
- 2.8. Retsmidler, ansvar og sanktioner
 - 2.8.1. Gældende ret
 - 2.8.2. Databeskyttelsesforordningen
 - 2.8.3. Justitsministeriets overvejelser og lovforslagets udformning

3. Økonomiske og administrative konsekvenser for det offentlige

4. Økonomiske og administrative konsekvenser for erhvervslivet mv.

5. Administrative konsekvenser for borgerne

6. Miljømæssige konsekvenser

7. Forholdet til EU-retten

8. Hørte myndigheder og organisationer mv.

9. Sammenfattende skema

1. Indledning

1.1. Baggrund og formål

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

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

Databeskyttelsesforordningen afløser direktiv 95/46/EF (databeskyttelsesdirektivet), som i dansk ret er gennemført ved persondataloven, jf. lov nr. 429 af 31. maj 2000 om behandling af personoplysninger, som senest ændret ved lov nr. 410 af 27. april 2017.

Databeskyttelsesforordningen vil have direkte virkning i Danmark, hvilket betyder, at der som udgangspunkt ikke må være anden dansk lovgivning, der regulerer behandling af personoplysninger, i det omfang dette er reguleret i forordningen.

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

Databeskyttelsesforordningen giver inden for en lang række områder mulighed for, at der i national ret kan fastsættes bestemmelser for at tilpasse anvendelsen af forordningen.

Justitsministeriet har vurderet, at det er nødvendigt, at der fastsættes en generel lov, som supplerer reglerne i databeskyttelsesforordningen. Dette er bl.a. nødvendigt for, at den gældende retstilstand så vidt muligt kan opretholdes, eksempelvis muligheden for at undtage oplysninger fra oplysningspligten og indsichtsretten samt muligheden for efter en række nærmere betingelser at behandle følsomme oplysninger.

Formålet med dette lovforslag er i en generel lov først og fremmest at supplere reglerne i databeskyttelsesforordningen. Forslaget fastsætter således supplerende nationale bestemmelser om behandling af personoplysninger inden for det nationale råderum, som databeskyttelsesforordningen giver mulighed for samtidig med, at den nugældende persondatalov ophæves.

Databeskyttelsesforordningen indeholder bestemmelser, hvorefter medlemsstaterne inden for nærmere bestemte områder enten *skal* eller *kan* fastsætte nationale regler.

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

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

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

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

Den sidste, *fjerde* kategori er bestemmelserne i forordningens artikel 43, stk. 1, artikel 51, stk. 1 og 3, artikel 52, stk. 2-4, artikel 53, stk. 1, artikel

54, stk. 1, artikel 84 og artikel 85, stk. 1 og 2, som skal gennemføres ved lov af medlemsstaterne. Efter artikel 51, stk. 1 og 3, skal medlemsstaterne eksempelvis fastsætte bestemmelser om udpegning eller oprettelse af en eller flere uafhængige tilsynsmyndigheder.

Lovforslagets formål er identisk med formålet i databeskyttelsesforordningen, nemlig beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og fri udveksling af personoplysninger i EU.

Justitsministeriet har den 24. maj 2017 udgivet betænkning nr. 1565/2017 om databeskyttelsesforordningen (*betænkningen*). *Betænkningen* indeholder to dele. Når der i lovforslaget henvises til *betænkningen* er det en henvisning til betænkningens del I, som indeholder en nærmere analyse af den gældende retstilstand og forordningens bestemmelser, herunder forordningens rammer for nationale særregler.

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

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

Betænkningens analyser danner grundlag for udarbejdelsen af dette lovforslag.

1.2. Lovforslagets indhold i hovedtræk

Lovforslaget er inddelt i afsnit om henholdsvis indledende bestemmelser, herunder anvendelses- og geografisk område (afsnit I), behandlingsregler, regler om videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige og kreditoplysningsbureauer (afsnit II), den registreredes rettigheder, herunder begrænsninger i den registreredes rettigheder (afsnit III), supplerende bestemmelser til databeskyttelsesforordningens kapitel IV, herunder tavshedspligt for databeskyttelsesrådgivere (afsnit IV), tilladelse til behandling (afsnit V), uafhængige tilsynsmyndigheder, herunder Datatilsynet og tilsyn med domstolene (afsnit VI) og retsmidler, ansvar og sanktioner, herunder afsluttende bestemmelser (afsnit VII).

Lovforslaget indeholder først og fremmest som supplement og sammen med databeskyttelsesforordningen de generelle regler for behandling af personoplysninger, som før den 25. maj 2018 alene fremgik af persondataloven. I den forbindelse henvises til forordningens præambelbetragtning nr. 8, hvorefter 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, kan indarbejde elementer af denne forordning i deres nationale ret.

Efter den 25. maj 2018 vil det herefter være reglerne i databeskyttelsesforordningen suppleret af lovforslaget, som – udover diverse danske særregler – regulerer området for behandling af personoplysninger.

Lovforslaget er i vidt omfang en videreførelse af de gældende regler i den nugældende persondatalov.

For så vidt angår anvendelsesområdet svarer dette i vidt omfang til den nugældende persondatalovs anvendelsesområde. Dog foreslås det i lovforslaget, at forslaget og databeskyttelsesforordningen skal finde anvendelse på Folketinget, når der ikke sker parlamentarisk arbejde og betjening.

Endvidere foreslås det i lovforslaget, at forslaget og databeskyttelsesforordningen skal finde anvendelse på *afdøde personer* i 10 år fra vedkommendes død samt en bemyndigelse til, at justitsministeren efter forhandling med vedkommende minister kan fastsætte regler om, at loven og forordningen skal finde anvendelse på afdøde personer i en længere eller kortere periode.

Lovforslagets anvendelsesområde indeholder endelig en ny version af den særlige danske ”krigsregel”.

For så vidt angår lovforslagets behandlingsregler, er der i vidt omfang tale om en videreførelse af de gældende regler, idet der dog indføres en særlig hjemmel for behandling i ansættelsesforhold. Dette afsnits formål er således særligt at udfylde og supplere databeskyttelsesforordningens behandlingsregler, så der i videst muligt omfang kan ske behandling i samme omfang, som det er tilfældet i dag. Derfor indeholder afsnittet en bestemmelse om genanvendelse, som sikrer, at der uanset reglerne i forordningen, er mulighed for, at vedkommende minister efter forhandling med justitsministeren kan bestemme, at der kan ske genanvendelse af oplysninger i så vidt muligt samme omfang som tidligere.

Endelig indeholder kapitlet en bestemmelse om *aldersgrænsen for børns samtykke* i forbindelse med udbud af informationssamfundstjenester.

For så vidt angår lovforslagets regler om den registreredes rettigheder, indeholder afsnittet en bestemmelse om muligheden for at begrænse den registreredes rettigheder, og for så vidt angår lovforslagets afsnit om supplerende bestemmelser til databeskyttelsesforordningen indeholder dette afsnit en bestemmelse om tavshedspligt for databeskyttelsesrådgivere.

For så vidt angår afsnittet om tilladelse til behandling, opretholdes tilladelsesordningen ved Datatilsynet vedrørende advarselsregistre, kreditoplysningsbureauer, retsinformationssystemer samt for behandling af følsomme oplysninger af hensyn til væsentlige samfundsinteresser (som dog reguleres i afsnittet om behandlingsregler). Det foreslås således i lovforslaget, at alle øvrige tidligere gældende ordninger om tilladelse og anmeldelse ikke opretholdes.

For så vidt angår de foreslåede regler om tilsynsmyndighederne, er der i vidt omfang tale om en videreførelse af gældende ret, herunder i forhold til kravet om uafhængighed og beskrivelsen af tilsynsmyndighedens opgaver.

For så vidt angår reglerne om retsmidler, ansvar og sanktioner, er der tale om dels en videreførelse af reglerne om adgangen til at klage til tilsynsmyndighederne og i et vist omfang adgangen til at indbringe tilsynsmyndighedens afgørelser for domstolene og dels en række nyskabelser, herunder i form af tilsynsmyndighedens adgang til at indbringe spørgsmål om overtrædelse af loven for domstolene.

1.3. Overordnet om den retlige ramme for lovforslaget i forhold til databeskyttelsesforordningen

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

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

Databeskyttelsesforordningen virker således som en lov i medlemsstaterne, og den gælder i den form, som den er vedtaget, og den må som udgangspunkt ikke gennemføres i national ret.

Ud over, at forordningen som udgangspunkt ikke må gennemføres i medlemsstaterne, vil medlemsstaternes modstridende lovgivning blive fortrængt af forordningen, hvorfor det vil være nødvendigt at ophæve denne lovgivning således, at der ikke opstår nogen usikkerhed om retstilstanden. Ophævelsen skal ske enten ved lov eller ved bekendtgørelse med hjemmel i lov. Forordningen vil således ikke i sig selv være en tilstrækkelig hjemmel til at ophæve lovgivning. Som følge heraf vil den nugældende persondatalov blive ophævet med lovforslaget.

Databeskyttelsesforordningens indhold forudsætter, at medlemsstaterne skal fastsætte nærmere regler, der gennemfører forordningens mere overordnede regulering. Databeskyttelsesforordningen dækker desuden langt fra hele det område, som den tidligere persondatalov dækkede. Som følge heraf gennemføres der en række danske særregler af mere generel og tværgående karakter i lovforslaget. Disse danske regler fastsættes mest hensigtsmæssigt i dette lovforslag.

Det har i forbindelse med udarbejdelsen af lovforslaget været nødvendigt at gengive dele af forordningen. EU-Domstolen anerkender, at en sådan gengivelse kan finde sted, blot det udtrykkeligt anføres i loven, at der er tale om en gengivelse af en forordning. I databeskyttelsesforordningens præambelbetragtning nr. 8 er det endvidere præciseret, at forordningens bestemmelser kan gengives i nationale regler, i det omfang det er nødvendigt af hensyn til sammenhængen og for at gøre de nationale bestemmelser forståelige for de personer, som de finder anvendelse på. I de tilfælde, hvor bestemmelser fra forordningen er gengivet i lovforslaget er dette af hensyn til at give et bedre overblik over den gældende retstilstand.

Endvidere er hele databeskyttelsesforordningen optrykt som bilag til lovforslaget.

2. Lovforslagets hovedpunkter

2.1. Lovens materielle anvendelsesområde

2.1.1. Gældende ret

Persondatalovens materielle anvendelsesområde fastlægges i lovens kapitel 1. Ifølge persondatalovens § 1, stk. 1, gælder loven således for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register. Bestemmelsen fastlægger lovens almindelige anvendelsesområde under hensyn til anvendelsesområdet i databeskyttelsesdirektivets artikel 3.

Af bestemmelsen i persondatalovens 1, stk. 2, følger, at loven gælder som udgangspunkt gælder for anden ikke-elektronisk systematisk behandling, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden.

Af bestemmelsen i persondatalovens § 1, stk. 3, følger, at lovens § 5, stk. 1-3, §§ 6-8, § 10, § 11, stk. 1, § 38 og § 40 gælder for *manuel videregivelse* af personoplysninger til en anden forvaltningsmyndighed.

Af bestemmelsen i persondatalovens § 1, stk. 4, følger, at persondataloven umiddelbart skal gælde for behandlinger, som udføres for kreditoplysningsbureauer, og som omfatter oplysninger om *virksomheder mv.*, samt at loven umiddelbart skal gælde med hensyn til private dataansvarliges behandling af oplysninger om *virksomheder mv.* med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til de pågældende virksomheder.

Af persondatalovens § 1, stk. 5, følger, at reglerne i lovens kapitel 5 gælder, uanset om der er tale om videregivelse af elektronisk behandlede oplysninger om videregivelse af oplysninger, der hidrører fra et manuelt register, jf. stk. 1.

I persondatalovens § 1, stk. 6, bemyndiges justitsministeren til at inddrage behandling af oplysninger om juridiske personer under lovens område.

Efter bestemmelsen i persondatalovens § 1, stk. 7, bemyndiges vedkommende minister til at inddrage behandling af oplysninger om juridiske personer under lovens område.

Af persondatalovens § 1, stk. 8, følger, at loven omfatter enhver form for behandling af personoplysninger i forbindelse med tv-overvågning.

Særligt for så vidt angår behandling af oplysninger om afdøde personer bemærkes det, at oplysninger om afdøde personer efter Datatilsynets praksis er omfattet af persondataloven, hvis der foreligger et særligt beskyttelsesbehov. Det kan f.eks. være tilfældet, hvis det drejer sig om følsomme oplysninger, herunder oplysninger om helbredsforhold, politisk overbevisning eller om strafbare forhold.

Persondatalovens § 2 indeholder en række undtagelser fra persondatalovens materielle anvendelsesområde.

Ifølge lovens § 2, stk. 1, går regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, forud for reglerne i persondataloven.

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

Endvidere følger det af persondatalovens § 2, stk. 2, at loven ikke finder anvendelse, hvis det vil være i strid med informations- og ytringsfriheden, jf. Den Europæiske Menneskerettighedskonventions artikel 10.

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

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

Derudover er der i persondatalovens § 2, stk. 5-9, en række undtagelser vedrørende mediernes behandling af oplysninger.

Endelig følger det af persondatalovens § 2, stk. 10, at loven ikke gælder for handlinger, der udføres for politiets og forsvarrets efterretningstjenester.

2.1.2. Databeskyttelsesforordningen

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

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

Bestemmelsen svarer således til det gældende databeskyttelsesdirektivs materielle anvendelsesområde.

Ligesom persondataloven gælder forordningen derfor også for domstolene.

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

I forordningens præambelbetragtning nr. 16 er det anført, at der herved er tale om aktiviteter *såsom* aktiviteter vedrørende statens sikkerhed. Eksemplet om statens sikkerhed må på samme måde som eksemplerne i databeskyttelsesdirektivets artikel 3, stk. 2, 1. pind, umiddelbart antages at fastlægge rækkevidden af undtagelsen i *litra a*, således at den alene finder anvendelse på aktiviteter, der kan henføres til statens sikkerhed, på trods af at ordet ”såsom” i præambelbetragtning nr. 16 ellers kunne antyde, at undtagelsen i *litra a* også omfattede andet end aktiviteter, der kan henføres til statens sikkerhed, jf. *betænkningen*, side 31-32.

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

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

Og endelig gælder forordningen efter artikel 2, stk. 2, *litra d*, ikke for behandling af personoplysninger, som foretages af *kompetente* myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafba-

re handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

Denne undtagelse vedrører forholdet til Europa-Parlamentets og Rådets direktiv (EU) 2016/680 (retshåndhævelsesdirektivet), som ifølge direktivets artikel 2, stk. 1, jf. § 1, stk. 1, finder anvendelse for sådanne handlinger. Retshåndhævelsesdirektivet er gennemført i dansk ret ved lov nr. 410 af 27. april 2017.

Om databeskyttelsesforordningens materielle anvendelsesområde henvises i øvrigt til *betænkningen*, side 31-34.

Særligt for så vidt angår afdøde personer fremgår det af forordningens præambelbetragtning nr. 27, at forordningen ikke finder anvendelse på personoplysninger om afdøde personer, men at medlemsstaterne kan fastsætte regler for behandling af personoplysninger om afdøde personer.

2.1.3. Justitsministeriets overvejelser og lovforslagets udformning

2.1.3.1. Databeskyttelsesforordningens materielle anvendelsesområde svarer i vidt omfang til den gældende ordning efter persondataloven.

Databeskyttelsesforordningens definitioner fremgår af forordningens artikel 4. De svarer i vidt omfang til definitionerne fra persondataloven, jf. lovens § 3. Definitionerne finder anvendelse på hele forordningens anvendelsesområde, herunder også i forhold til nærværende lovforslag.

Ordningen vedrørende persondatalovens *materielle* anvendelsesområde er, at *al* elektronisk behandling af personoplysninger er omfattet af loven, jf. nærmere § 1, stk. 1, *medmindre* behandlingen undtages fra loven i § 2, såsom § 2, stk. 10, hvorefter loven ikke gælder for handlinger, der udføres for politiets og forsvarets efterretningstjenester. Sidstnævnte ligger inden for rammerne af undtagelsesmuligheden i databeskyttelsesdirektivets artikel 3, stk. 2, 1. pind, hvorefter direktivet ikke finder anvendelse på behandling af personoplysninger, som iværksættes med henblik på udøvelse af aktiviteter af hensyn til statens sikkerhed.

Justitsministeriet finder, at lovforslaget skal følge samme fremgangsmåde således, at det heri reguleres, at lovforslaget og databeskyttelsesforordningen finder anvendelse på *al* behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling og på anden ikke-

automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, *medmindre* lovforslaget udtrykkeligt undtager nærmere bestemte former for anvendelse af personoplysninger.

Denne fremgangsmåde er valgt, så det bliver slået fast, at forordningen vil gælde på alle livsområder med undtagelse af aktiviteter vedrørende statens sikkerhed efter artikel 2, stk. 2, litra a, og de øvrige områder, der er nævnt i forordningens artikel 2, stk. 2, litra b-d.

På den måde sikres det, at en eventuel fortolkningstvivl vedrørende forordningens artikel 2, stk. 2, litra a, ryddes af vejen ved, at forordningens artikel 2, stk. 2, litra a, *alene* anvendes på aktiviteter vedrørende statens sikkerhed.

Fremgangsmåden vil således sikre, at *al* automatisk behandling af personoplysninger som udgangspunkt er omfattet af lovforslaget, medmindre behandlingen er undtaget som følge af artikel 2, stk. 2, litra b-d, eller i lovforslagets § 3, der dels indeholder undtagelser af hensyn til statens sikkerhed, såsom § 3, stk. 2, om politiets og forsvarrets efterretningstjenester (udnyttelse af forordningens artikel 2, stk. 2, litra a) og dels indeholder en udnyttelse af muligheden i forordningens artikel 85 til ved lov at forene retten til beskyttelse af personoplysninger med retten til ytrings- og informationsfrihed.

2.1.3.2. Persondatalovens øvrige materielle anvendelsesområde, jf. lovens § 1, stk. 2-7, vedrører hovedsagligt forhold, som falder uden for forordningens anvendelsesområde, fordi de nævnte bestemmelser regulerer ikke-elektronisk behandling af personoplysninger.

Forordningen vil ikke være til hinder for, at der opretholdes sådanne tilsvarende regler inden for dette anvendelsesområde. Det samme gælder for persondatalovens § 1, stk. 8, om behandling af personoplysninger i forbindelse med tv-overvågning, idet omfang der er tale om brug af analogt tv-overvågningsudstyr.

Justitsministeriet finder, at der på en række af de områder, der i dag er omfattet af persondatalovens § 1, stk. 2-8, også i fremtiden bør være en databeskyttelsesretlig regulering.

Som anført ovenfor under beskrivelsen af gældende ret, finder persondataloven anvendelse for visse ikke-elektroniske systematiske behandlinger,

som udføres for private. I takt med den teknologiske udvikling har denne bestemmelse et meget begrænset anvendelsesområde. I lyset heraf, samt henset til harmoniseringshensyn, har Justitsministeriet ikke fundet det hensigtsmæssigt at foreslå en tilsvarende bestemmelse i det foreliggende lovforslag.

Særligt for så vidt angår oplysninger om afdøde personer, finder Justitsministeriet, at hensynet til, at oplysninger om afdøde personer kan være af væsentlig betydning for de afdødes eftermæle og dermed også for de nulevende pårørende, begrundet, at oplysninger om afdøde i en vis periode bør været omfattet af den beskyttelse, der følger af lovforslaget og forordningen. Det foreslås derfor, at lovforslaget skal finde anvendelse for oplysninger om afdøde personer i 10 år efter vedkommendes død. Dermed fastslås den gældende praksis fra Datatilsynet i lovforslaget, dog med den tilføjelse, at der indføres en tidsbegrænsning på 10 år. Samtidig foreslås det, at der kan fastsættes regler om, at lovforslaget og forordningen skal finde anvendelse på oplysninger om afdøde personer i en kortere eller længere periode end 10 år.

Perioden på 10 år er valgt ud fra, at denne periode i de fleste tilfælde vil kunne være passende ud fra de ovenfor nævnte hensyn. Samtidig vil en præcis angivelse af en tidsperiode gøre reglen nemmere at administrere i praksis.

Der henvises i øvrigt til de specielle bemærkninger til lovforslagets § 2, hvorefter lovforslagets og databeskyttelsesforordningens anvendelsesområde fastlægges og udvides til at omfatte behandling af oplysninger, som ikke uden videre er omfattet af forordningens anvendelsesområde.

2.2. Lovens geografiske anvendelsesområde

2.2.1. Gældende ret

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

Bestemmelsen omfatter kun dataansvarlige etableret på dansk område.

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

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

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

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

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

Om persondatalovens territoriale anvendelsesområde henvises i øvrigt til *betænkningen*, side 29-30.

2.2.2. Databeskyttelsesforordningen

2.2.2.1. Databeskyttelsesforordningens territoriale anvendelsesområde reguleres i artikel 3, stk. 1, hvorefter den 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. Bestemmelsen har - ligesom databeskyttelsesdirektivets artikel 4 - karakter af en lovvalgsregel.

Ifølge artikel 3, stk. 2, *litra a*, finder forordningen endvidere anvendelse på behandling af personoplysninger om registrerede, der er i Unionen, og som foretages af en dataansvarlig eller databehandler, der *ikke* er etableret i

Unionen, hvis behandlingsaktiviteterne vedrører udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet.

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

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

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

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

Om databeskyttelsesforordningens territoriale anvendelsesområde henvises i øvrigt til *betænkningen*, side 34-37.

2.2.3. Justitsministeriets overvejelser og lovforslagets udformning

2.2.3.3. Databeskyttelsesforordningens territoriale anvendelsesområde svarer i vidt omfang til den gældende ordning efter persondataloven.

Persondatalovens *territoriale* anvendelsesområde bygger først og fremmest på, at den finder anvendelse, hvis den *dataansvarlige* er *etableret* i

Danmark, hvis aktiviteterne finder sted inden for EU, jf. lovens § 4, stk. 1, og afsnit 2.2.1. ovenfor.

Forordningen bygger på samme kriterium om etablering ved i artikel 3, stk. 1, at bestemme, at forordningen 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.

Forordningen tager ikke stilling til, hvornår den nationale lovgivning, som medlemsstaterne vedtager indenfor rammerne af forordningen – f.eks. i medfør af artikel 6, stk. 2-3, artikel 8, stk. 1, artikel 9, stk. 4, og artikel 89 – skal finde anvendelse. Man vil om denne nationale lovgivning, vedtaget indenfor rammerne af forordningen, formentlig se, at medlemsstaterne vælger forskellige tilgange, således, at nogle medlemslande vil lade det være afgørende, hvor den registrerede har bopæl eller befinder sig, mens andre medlemslande – forventeligt de fleste – vil lade det være afgørende, hvor den dataansvarlige eller databehandlere, der er underlagt den pågældende nationale lovgivning, er etableret.

Justitsministeriet finder det mest nærliggende at lade lovforslaget gælde for dataansvarlige og databehandlere, der er *etableret* i Danmark. Hermed følges den ordning, der er kendes i dag fra persondatalovens § 4, stk. 1.

Herudover foreslås det, at danske diplomatiske repræsentationer skal være omfattet af lovforslaget. Diplomatiske repræsentationer, der efter folkeretten er forpligtet til at overholde modtagerlandets lovgivning, nyder som udgangspunkt immunitet i modtager staten med hensyn til søgsmål og eksekution. Med en bestemmelse, som udstrækker lovforslaget til også at gælde for danske diplomatiske repræsentationer, sikres det således, at tilsynet med danske diplomatiske repræsentationer foretaget af Datatilsynet.

Der henvises i øvrigt til lovforslagets § 4 og de specielle bemærkninger hertil.

For den øvrige danske særregulering, der omfattes af forordningens materielle anvendelsesområde, må det territoriale anvendelsesområde afgøres på baggrund af den pågældende lovgivning.

Reglerne i lovforslaget og databeskyttelsesforordningens artikel 3 berører ikke spørgsmålet om strafferetlig jurisdiktionskompetence. Dette spørgsmål afgøres - ligesom i dag - efter reglerne i straffelovens kapitel 2.

2.3. Behandlingsregler

2.3.1. Formålsbestemthed

2.3.1.1. Gældende ret

I persondatalovens § 5 er fastsat en række grundlæggende principper for den dataansvarliges behandling af oplysninger, som altid skal iagttages. Reglerne giver ikke den dataansvarlige et selvstændigt grundlag for at foretage en bestemt behandling af oplysninger. Hjemmel hertil skal søges i de øvrige behandlingsregler i persondatalovens §§ 6-13, kapitel 5-7 eller eventuelt i særlovgivningen.

Det følger af persondatalovens § 5, stk. 2, at indsamlede oplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål (finalité-princippet).

Efter bestemmelsen må senere behandling af oplysninger ikke være uforenelig med de formål, hvortil oplysningerne er indsamlet. Bestemmelsen indebærer, at de oplysninger, som den dataansvarlige måtte indsamle, ikke frit vil kunne genbruges, videregives m.v. Der vil således heller ikke frit kunne videregives oplysninger inden for f.eks. den offentlige forvaltning. I det omfang, genbrug, udveksling m.v. ikke er uforenelig med det eller de formål, hvortil oplysningerne er indsamlet af den dataansvarlige, vil der dog være mulighed herfor. I hvilket omfang dette er tilfældet, vil bero på en konkret vurdering i den enkelte situation. Det bemærkes, at behandling til andre formål end de formål, hvortil oplysningerne oprindeligt er indsamlet, naturligvis skal ske i overensstemmelse med de materielle regler i §§ 6-13 og i kapitel 5-7. Videregivelse af indsamlede oplysninger til tredjemand skal således være lovlig efter de materielle regler i §§ 6-13, og videregivelsen må ikke være uforenelig med de formål, som oplysningerne er indsamlet til. Det vil derfor ikke være muligt at omgå reglerne ved, at den dataansvarlige videregiver oplysningerne til en tredjemand, som ved sin indsamling af oplysningerne fastsætter formål, som er uforenelige med de formål, hvortil oplysningerne oprindeligt er indsamlet af den dataansvarlige. Derimod er bestemmelsen ikke til hinder for, at den registrerede meddeler sit samtykke til, at de indsamlede oplysninger behandles til formål, der er uforenelige med de formål, hvortil oplysningerne oprin-

delig er indsamlet. En sådan situation er at sidestille med en fornyet indsamling af de pågældende oplysninger.

2.3.1.2. Databeskyttelsesforordningen

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

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

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

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

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

Det fremgår således af forordningens artikel 6, stk. 4, 2. led, litra a-e, og præambelbetragtning nr. 50, 1. afsnit, 5. pkt., at for at afgøre om et andet behandlingsformål er foreneligt med det formål, som personoplysningerne

oprindeligt blev indsamlet til, skal den dataansvarlige bl.a. tage hensyn til enhver forbindelse mellem det formål, som personoplysningerne er indsamlet til og formålet med den påtænkte viderebehandling, den sammenhæng, hvori personoplysningerne er blevet indsamlet, navnlig med hensyn til forholdet mellem den registrerede og den dataansvarlige, personoplysningernes art, navnlig om særlige kategorier af personoplysninger behandles, jf. artikel 9, eller om personoplysninger vedrørende straffedomme og lovovertrædelser behandles, jf. artikel 10, den påtænkte viderebehandlings mulige konsekvenser for de registrerede og tilstedeværelse af fornødne garantier, som kan omfatte kryptering eller pseudonymisering.

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

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

Disse tre muligheder for genanvendelse af personoplysninger til nye formål gennemgås nærmere i *betænkningen*, side 94-97.

Alt i alt skal en eventuel viderebehandling til nye formål – hvis den ikke bygger på samtykke eller er bestemt i EU-retten eller medlemsstaternes nationale ret leve op til den ovenfor omtalte ”test” om, hvorvidt det nye formål er uforeneligt med det oprindelige artikel 6, stk. 4, litra a-e. Anvendelsen af denne test forudsætter i udgangspunktet en konkretiseret vurdering.

2.3.1.3. Justitsministeriets overvejelser og lovforslagets udformning

Som anført ovenfor under beskrivelsen af forordningen vil der inden for rammerne af forordningen være mulighed for uden samtykke eller uden specifik hjemmel i EU-retten eller national ret, at videreanvende oplysninger.

Regeringen ønsker, at det offentlige kan videreanvende og genbrugedata på en effektiv, åben og transparent måde, der stadig lever op til kravene om databeskyttelse.

Samtidig skal der skabes rammer for en effektiv datadeling, så borgerne og virksomhederne kan få en mere effektiv sagsbehandling og mere målrettede, sammenhængende indsatser, der virker bedre for den enkelte.

Med lovforslaget lægges der derfor op til at tydeliggøre den adgang til videreanvendelse og genbrug af oplysninger, som følger af forordningen, ved at fastsætte en særlig bestemmelse om formålsbestemthed. Der fastsættes desuden en bemyndigelsesbestemmelse, hvorefter vedkommende minister efter forhandling med justitsministeren, inden for rammerne i databeskyttelsesforordningen, i bekendtgørelsesform kan bestemme, at personoplysninger må viderebehandles til andre formål, end de oprindeligt var indsamlet til, uafhængigt af formålenes forenelighed.

Dette vil bidrage til at skabe mere åbenhed for borgerne, når de på forhånd vil kunne orientere sig i, om en given viderebehandling kan ske til andet formål end det oprindelige, ligesom det set fra myndigheds side skal et sikkert retligt grundlag på forhånd for, om viderebehandlingen kan ske.

Der henvises til bemærkningerne til lovforslagets § 5, stk. 3.

2.3.2. Behandling af almindelige oplysninger

2.3.2.1. Gældende ret

I *betænkningen*, særligt side 81-92, 113-127 og 195-208, er der givet en redegørelse for persondatalovens regler om behandlingen af *almindelige* personoplysninger, omfattet af lovens § 6, *særlige kategorier* af personoplysninger, omfattet af lovens §§ 7-8 og de generelle principper for behandling af personoplysninger i lovens § 5, som skal være opfyldt ved enhver behandling af personoplysninger.

Der redegøres derfor i det følgende kun for hovedtrækkene i disse regler.

I persondatalovens § 5 er fastsat en række generelle principper for den dataansvarliges behandling af oplysninger, som skal være opfyldt ved al behandling af personoplysninger. Disse principper skal ses i sammenhæng med bestemmelserne i §§ 6-13, hvori de nærmere betingelser for behandling af oplysninger er fastsat. Lovligheden af behandling af oplysninger

skal som udgangspunkt bedømmes efter reglerne i § 6. Dette gælder dog ikke, hvis der er tale om behandling af særlige oplysningstyper, jf. § 7 om en række følsomme personoplysninger, såsom helbredsoplysninger, og § 8 om oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold. For særlige former for behandling af oplysninger finder lovens §§ 9-13 anvendelse. Disse bestemmelser omhandler behandling af personnumre og personoplysninger i forbindelse med bl.a. retsinformationssystemer samt forskning og statistik. I persondatalovens § 14 er der endelig fastsat regler om arkivering af oplysninger, der er omfattet af loven.

Reglerne i persondatalovens § 6-13 finder som udgangspunkt anvendelse på al behandling af oplysninger. I det omfang, der er tale om særlige former for behandling, gælder dog reglerne i kapitel 5-7 om henholdsvis videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige, kreditoplysningsbureauer og om overførsel af oplysninger til tredjelande. Kun i de tilfælde, hvor der opstår spørgsmål, som ikke er reguleret i kapitel 5-7, vil finder de almindelige behandlingsregler således anvendelse på de nævnte særlige former for behandling af oplysninger. Ved overførsel af oplysninger til tredjelande, jf. kapitel 7, vil de almindelige betingelser dog skulle være opfyldt, jf. § 27, stk. 5.

Almindelige personoplysninger, omfattet af persondatalovens § 6, kan efter dennes stk. 1 behandles på betingelse af, at den registrerede har givet sit samtykke hertil, at behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en sådan aftale, at behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, at behandlingen er nødvendig for at beskytte den registreredes vitale interesser, at behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse, at behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt, eller at behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse.

Persondatalovens § 8 lægger rammerne for det offentliges og privates adgang til at behandle personoplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold.

Idet angivelsen af følsomme oplysninger, der er fastsat i direktivets artikel 8, stk. 1, som persondatalovens § 7 om følsomme oplysninger er baseret på, er udtømmende, var det ikke muligt at indsætte bl.a. ”væsentlige sociale problemer”, ”rent private forhold og ”strafbare forhold” i opregningen af følsomme oplysninger i persondatalovens § 7, stk. 1.

Justitsministeriet gav imidlertid i bemærkningerne til det tidligere lovfor-slag til persondataloven (nr. L 44 af 8. oktober 1998) og i svar til Folketin-gets Retsudvalg udtryk for, at det var en forudsætning, at de almindelige behandlingsregler i lovforslagets §§ 6 og 7 i videst muligt omfang skulle administreres således, at der ikke – uden samtykke – kunne registreres og videregives personoplysninger i videre udstrækning end efter registerlove-ne. En sådan administration måtte efter Justitsministeriets opfattelse anta-ges at falde inden for rammerne af direktivet.

Persondatalovens § 8 har således til formål at udgøre en del af den samlede danske gennemførelse af databeskyttelsesdirektivets – mindre restriktive – regler for behandling af andre typer af oplysninger.

Det skyldes, at direktivet overlader medlemsstaterne et vist spillerum til at fastlægge de nærmere kriterier for adgangen til at behandle oplysninger, der ikke – i direktivets forstand – har karakter af særligt følsomme oplysninger.

Det følger af persondatalovens § 8, stk. 3, at forvaltningsmyndigheder, der udfører opgaver inden for det sociale område, kun må videregive de i stk. 1 nævnte oplysninger og de oplysninger der er nævnt i § 7, stk. 1, hvis betingelserne i stk. 2, nr. 1 eller 2 er opfyldt, eller hvis videregivelsen er et nødvendigt led i sagens behandling eller nødvendig for, at en myndighed kan gennemføre tilsyns- eller kontrolopgaver.

Bestemmelsen i stk. 3 begrænser inden for det sociale område den adgang til at videregive oplysninger om rent private forhold, som følger dels af den forudsatte administration af de almindelige behandlingsregler i person-datalovens § 7 (med hensyn til de i § 7, stk. 1, angivne oplysninger om rent private forhold), dels af stk. 2 (med hensyn til øvrige oplysninger om rent private forhold).

I persondatalovens § 13 er der fastsat regler for offentlige myndigheds og private virksomheders mv. adgang til at foretage automatisk registrering af, hvilke telefonnumre, der er foretages opfald til fra deres telefoner.

Reglen tager sigte på at beskytte ansattes privatliv i forbindelse med brugen af telefoner, som er installeret hos den ansattes arbejdsgiver, det være sig offentlige myndigheder eller private virksomheder mv. Baggrunden for bestemmelsen er, at der i Danmark – på tidspunktet for fremsættelsen af persondataloven – var tradition for, at ansatte i et vist omfang kunne benytte telefoner på arbejdspladser til private formål.

2.3.2.2. Databeskyttelsesforordningen

Databeskyttelsesforordningen indeholder samme sondring mellem hjemmel til behandling af almindelige personoplysninger i artikel 6, stk. 1, der i vidt omfang svarer til persondatalovens § 6, stk. 1, og følsomme personoplysninger omfattet artikel 9, der bærer overskriften "[b]ehandling af særlige kategorier af personoplysninger", om som i vidt omfang svarer til persondatalovens § 7.

Herudover følger der en række grundlæggende principper af databeskyttelsesforordningens artikel 5, stk. 1, der skal være opfyldt ved al behandling af personoplysninger. Principperne svarer til persondatalovens § 5, stk. 1, og databeskyttelsesdirektivets artikel 6, stk. 1.

Der henvises til *betænkningen*, særligt side 92-101, side 127-140 og side 191-194, side 208-227, for en gennemgang af de muligheder forordningen rummer for at behandle personoplysninger.

Der redegøres derfor i det følgende kun for hovedtrækkene i forordningens nye behandlingsregler.

Det kan på den baggrund nævnes, at almindelige personoplysninger, omfattet af forordningens artikel 6, således efter bestemmelsens stk. 1 kan behandles på betingelse af, at den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål (litra a), at 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 (litra b), at behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige (litra c), at behandling er

nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser (litra d), at 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 (litra e), eller at 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 (litra a). Denne sidste mulighed gælder – som noget nyt i forhold til den gældende retstilstand – ikke for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver, jf. artikel 6, stk. 1, litra f, 2. afsnit. Der kan i den forbindelse henvises til *betænkningen*, side 139-141, hvoraf det bl.a. fremgår, at det ikke kan antages at være hensigten med forordningen at begrænse offentlige myndigheders mulighed for at behandle personoplysninger, og at hjemmel til behandling af personoplysninger for offentlige myndigheder som led i udførelsen af deres opgaver, vil skulle findes i de øvrige behandlingshjemler i forordningens artikel 6, stk. 1, særligt artikel 6, stk. 1, litra c og e.

Databeskyttelsesforordningens artikel 6, stk. 1, litra a-f, opregnede behandlingsmuligheder kan anvendes som direkte behandlingshjemler, så længe behandlingsbetingelserne i de pågældende bestemmelser er opfyldt. Det må således antages, at f.eks. artikel 6, stk. 1, litra c, er direkte anvendelig som behandlingsgrundlag, når blot den retlige forpligtelse følger af f.eks. national ret. Brugen af f.eks. artikel 6, stk. 1, litra c, som behandlingsgrundlag forudsætter således ikke en national, implementerende hjemmelslovgivning om selve den konkrete behandling af personoplysninger i forbindelse med fastlæggelsen af en retlig forpligtelse. Der henvises til *betænkningen* side 130 f. og side 132.

Artikel 8 i forordningen indeholder nye regler for et barns samtykke i forbindelse med informationssamfundstjenester. I artikel 8, stk. 1, efterlades medlemsstaterne en mulighed for ved lov at fastsætte en lavere aldersgrænse end 16 år, dog ikke under 13 år. Der henvises til *betænkningen* side 185-189.

2.3.2.3. *Justitsministeriets overvejelser og lovforslagets udformning*

Det er Justitsministeriets vurdering, at der i meget vidt omfang efter databeskyttelsesforordningens artikel 6 vil kunne behandles *almindelige oplysninger* i samme omfang som det er tilfælde i dag efter persondatalovens § 6, der bygger på databeskyttelsesdirektivets artikel 7. Der henvises til det

ovenfor anførte om mulighederne for at behandle oplysninger efter forordningens artikel 6.

Særligt om samtykke til behandling af personoplysninger i forbindelse med informationssamfundstjenester, giver forordningen som anført ovenfor mulighed for at fastsætte regler om en lavere aldersgrænse end 16 år.

Børn i Danmark er i høj grad medievanter. Adgang til information via søgemaskiner og deltagelse i online aktiviteter har stor samfundsmæssig og social betydning for børn og unge. Aktiviteter i denne sammenhæng er med til at skabe og fastholde kontakt med kammerater, deltage i forskellige diskussionsfora, søge information til skolearbejde, spille spil, se film og lytte til musik.

En høj aldersgrænse for, hvornår et barn gyldigt kan give samtykke til behandling af personoplysninger kan føre til, at børn og unge udelukkes fra informationssamfundstjenester, hvis forældremyndighedsindehaveren ikke vil give samtykke til behandling af personoplysninger. Denne uønskede effekt må opvejes imod den integritetsbeskyttelse, som en høj aldersgrænse måtte give. Man kunne også forestille sig, at en høj aldersgrænse ville medføre, at børn og unge ved brug af informationssamfundstjenester udgiver sig for at være ældre, end de rent faktisk er. Der kan også peges på, at børn og unge gennem databeskyttelsesforordningen og gennem lovforslagets bestemmelser – uanset et krav om samtykke fra forældremyndighedsindehaverne – ydes en integritetsbeskyttelse. Det er således tvivlsomt, om en høj aldersgrænse for samtykke medfører en øget integritetsbeskyttelse.

Samlet set er det derfor Justitsministeriets vurdering, at der ikke bør gælde en høj aldersgrænse for børns samtykke i forbindelse med udbud af informationssamfundstjenester.

Justitsministeriet foreslår derfor, at der fastsættes den laveste aldersgrænse, som forordningen tillader. Det foreslås derfor, at der fastsættes en aldersgrænse for børns samtykke til anvendelse af informationssamfundstjenester på 13 år.

For så vidt angår den nuværende regulering efter persondatalovens § 8 om det offentlige og det private behandling af oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold, er det Justitsministeriet vurdering, at bestemmelsen skal opretholdes også i fremtiden for så vidt angår behandling af oplysninger om strafbare forhold. Der

henvises i den forbindelse *betænkningen*, side 247-248, hvor muligheder for at opretholde reguleringen i persondatalovens § 8 om behandling af oplysninger om strafbare forhold er behandlet.

For så vidt angår den del af persondatalovens § 8, der vedrører behandling af oplysninger om væsentlige sociale problemer og andre rent private forhold bemærkes det, at sådanne oplysninger ikke omfattes af forordningens udtømmende liste over følsomme oplysninger i artikel 9. Sådanne oplysninger omfattes således af artikel 6 om almindelige oplysninger. Der er således ikke for så vidt angår oplysninger om væsentlige sociale problemer og andre rent private forhold en særlig regulering heraf i forordningen – i modsætning til oplysninger om strafbare forhold, der omfattes af forordningens artikel 10. Der henvises til *betænkningen* side 233-248.

Det er Justitsministeriets vurdering, at behandling af oplysninger om væsentlige sociale problemer og andre rent private forhold fremover skal kunne foretages (alene) på baggrund af behandlingsreglerne i forordningens artikel 6, jf. artikel 5.

Det er ikke hermed hensigten, at beskyttelsesniveauet sænkes for behandling af oplysninger om væsentlige sociale problemer og andre rent private forhold. Det bemærkes i den forbindelse, at det ved brug af behandlingsgrundlagene i artikel 6, stk. 1, i vid udstrækning er afgørende, om behandling af oplysninger er *nødvendig* til varetagelse af de i bestemmelsen opregnede interesser. I hvilket omfang, dette er tilfældet, vil bero på den konkrete situation. Der vil således med kravet om nødvendighed være overladt den dataansvarlige et vist skøn, som dog altid vil kunne efterprøves af tilsynsmyndigheden. Hertil kommer, at al behandling af personoplysninger skal leve op til artikel 5, herunder dataminimeringsprincippet i stk. 1, litra c, hvorefter personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles – altså et krav om proportionalitet.

Behandling af oplysninger om væsentlige sociale problemer og andre rent private forhold, der i dag er omfattet af persondatalovens § 8, vil alt andet lige stille skærpede krav til proportionalitetsvurderingen i forbindelse med behandlingen fremover efter forordningens artikel 6, jf. artikel 5, og det er på den baggrund, Justitsministeriets vurdering, at beskyttelsesniveauet ikke reelt sænkes for behandling af oplysninger om væsentlige sociale problemer og andre rent private forhold, selvom behandling af sådanne oplys-

ninger ikke fremover vil være omfattet af en særregulering svarende til persondatalovens § 8.

Det bemærkes, at der ikke er fundet behov for at medtage en bestemmelse svarende til persondatalovens § 8, stk. 3. Baggrunden er, at § 8, stk. 3, i dag er blevet udvandet af særlovgivningen, der fraviger bestemmelsen på en lang række områder. Bestemmelsen må derfor anses for i dag at have et yderst begrænset anvendelsesområde. Dette skal endvidere ses i lyset af, at persondatalovens § 8 alene foreslås opretholdt for så vidt angår oplysninger om strafbare forhold.

Samkøring er en fælles betegnelse for forskellige tekniske løsninger, som vedrører sammenkobling af oplysninger, der kommer fra forskellige registersystemer. Der kan blandt andet være tale om maskinelle overførsler, hvorved et register tilføres oplysninger fra et andet register, således at det modtagne register udvides med disse oplysninger, eller maskinelle sammenstillinger af oplysninger fra forskellige registre, hvorved der dannes et nyt uddataprodukt, eksempelvis et nyt register.

Samkøring af personoplysninger i *kontroløjemed* kræver efter dansk ret særskilt lovhjemmel. Det følger af en tilkendegivelse fra Retsudvalgets flertal i betænkningen over lovforslag nr. L 50 af 16. januar 1991 om ændring af lov om offentlige myndigheders registre og tidligere praksis fra Registertilsynet, som er videreført af Datatilsynet, at der ved samkøring i kontroløjemed stilles krav om, at en sådan samkøring sker på et klart og utvetydigt retsgrundlag, hvilket i praksis vil sige på grundlag af direkte lovhjemmel, ligesom der stilles krav om, at de berørte personer har fået meddelelse om kontrollen, inden de afgiver oplysninger til myndigheden.

Som eksempel på lovhjemmel til samkøring i kontroløjemed kan nævnes § 11 a, stk. 2, i lov om retssikkerhed på det sociale område, jf. lovbekendtgørelse nr. 1052 af 8. september 2015 med senere ændringer, og § 12 i lov om Udbetaling Danmark, jf. lovbekendtgørelse nr. 1507 af 6. december 2016.

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

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

Databeskyttelsesdirektivet pålagde heller ikke medlemsstaterne sådanne krav.

Efter databeskyttelsesforordningen vil samkøring i kontroløjemed således skulle leve op til de almindelige principper og regler om behandling. Da samkøring i kontroløjemed per definition vil være en indgribende behandlingssituation, vil sådan behandling dog skærpe opmærksomheden på kravene i blandt andet forordningens artikel 5 om principper for behandling af personoplysninger, herunder proportionalitetsprincippet. Der henvises om samkøring i kontroløjemed til *betænkningen*, side 86-87 og side 96-97.

Det er med dette lovforslag *ikke* længere en forudsætning, at samkøring i kontroløjemed skal have hjemmel særskilt i en lov. Det er således Justitsministeriets vurdering, at særligt databeskyttelsesforordningens artikel 5 og artikel 6, stk. 4, om principper for behandling af personoplysninger, herunder proportionalitetsprincippet og princippet om formålsbegrænsning, yder en tilstrækkelig stærk beskyttelse til de registrerede samtidigt med, at forordningens sikrer rum for offentlige myndigheders saglige behov for at kunne samkøre personoplysninger i kontroløjemed. Om det to fremhævede principper i forordningens artikel 5 og artikel 6, stk. 4, henvises til *betænkningen*, side 93-99.

Det har været overvejet i hvilket omfang offentlige myndigheder kan *offentliggøre kontrol- og analyseresultater og afgørelser* mv. om personer og/eller virksomheder i identificerbar form. Denne form for offentliggørelse – der i stigende grad sker via internettet – omfatter i mange tilfælde oplysninger, der ellers ville være fortrolige, herunder oplysninger om f.eks. personer eller virksomheder, der ikke har overholdt regler fastsat i lovgivningen.

Det vurderes i betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv., at reglerne i persondataloven fører til, at der kun kan etableres ordninger med systematisk offent-

liggørelse af kontrolresultater, afgørelser mv. i ikke-anonymiseret form, hvis der er særlig og klar lovhjemmel hertil.

Efter databeskyttelsesforordningen er der ikke et udtrykkeligt krav om, at der skal være udtrykkelig lovhjemmel for, at der kan etableres en ordning med systematisk offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke-anonymiseret form.

Da offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke-anonymiseret form vil være en indgribende behandlingssituation, vil sådan behandling dog skærpe opmærksomheden på kravene i blandt andet forordningens artikel 5 om principper for behandling af personoplysninger, herunder proportionalitetsprincippet.²

Databeskyttelsesforordningen ses ikke at ændre afgørende ved den beskrevne retsstilling i betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. Det må således også efter databeskyttelsesforordningen antages, at det skaber det sikreste behandlingsgrundlag for systematisk offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke-anonymiseret form, hvis der ligger en særlig og klar national lovhjemmel til grund for offentliggørelsen – udarbejdet i overensstemmelse med forordningens rammer for national lovgivning, jf. bl.a. artikel 6, stk. 2-3.

Uanset forordningen må det antages, at det er muligt at operere med en forudsætning om, at der skal ligge en særlig og klar lovhjemmel til grund for systematisk offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke-anonymiseret form.

Der henvises om offentlige myndigheder kan offentliggøre kontrol- og analyseresultater og afgørelser mv. nærmere til *betænkningen*, side 163-166.

Det er på den baggrund med dette lovforslag *fortsat* en forudsætning, at der skal ligge en særlig og klar lovhjemmel til grund for systematisk offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke-anonymiseret form.

² Dette følger også af EU-Domstolens afgørelse i sag C-92/09 og C-93/09, Volker und Markus Schecke GbR & Hartmut Eifert.

Dette skal ses i lyset af, at der er tale om en meget indgribende behandling af personoplysninger.

Det efter Justitsministeriets opfattelse vanskeligt at se behovet i dag for at opretholde persondatalovens § 13 om offentlige myndigheder og private virksomheders manglende mulighed for at foretage *automatisk registrering* af, hvilke *telefonnumre* der er foretaget opkald til fra deres telefoner. Dette begrundes navnlig i, at offentlige myndigheder og private virksomheder, som stiller telefoner til rådighed, i forbindelse med en eventuel automatisk registrering vil skulle overholde reglerne i lovforslaget og forordningen, hvilket må anses for at yde en tilstrækkelig integritetsbeskyttelse, herunder også henset til karakteren af de pågældende oplysninger.

Der er på den baggrund ikke medtaget regler svarende til persondatalovens § 13 i lovforslaget.

Der henvises til bemærkningerne til lovforslagets § 6.

2.3.3. Behandling af følsomme oplysninger

2.3.3.1. Gældende ret

Følsomme oplysninger omfattet af persondatalovens § 7 må som udgangspunkt ikke behandles. Det drejer sig om oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

De følsomme oplysninger omfattet af § 7 må dog behandles, hvis der er hjemmel til det i loven. Behandling af de pågældende oplysninger kan således ske på betingelse af, at den registrerede har givet sit udtrykkelige samtykke til en sådan behandling, at behandlingen er nødvendig for at beskytte den registreredes eller en anden persons vitale interesser i tilfælde, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke, at behandlingen vedrører oplysninger, som er blevet offentliggjort af den registrerede, eller at behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares, jf. persondatalovens § 7, stk. 2.

Endvidere kan behandling af oplysninger om fagforeningsmæssige tilhørsforhold skal kunne ske, hvis behandlingen er nødvendig for overholdelsen af den dataansvarliges arbejdsretlige forpligtelser eller specifikke rettigheder, jf. lovens § 7, stk. 3.

Herudover kan en stiftelse, en forening eller en anden almennyttig organisation, hvis sigte er af politisk, filosofisk, religiøs eller faglig art, inden for rammerne af sin virksomhed foretage behandling af oplysninger omfattet af § 7 om organisationens medlemmer eller personer, der på grund af organisationens formål er i regelmæssig kontakt med denne, jf. lovens § 7, stk. 4.

Er der tale om behandling af særlige kategorier af oplysninger, der er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, kan dette også kunne ske, hvis behandlingen af oplysningerne foretages af en person, der efter lovgivningen er undergivet tavshedspligt, jf. lovens § 7, stk. 5. Bestemmelsen, der vedrører behandling af personoplysninger inden for sundhedssektoren, suppleres af reglerne i sundhedsloven, der i kapitel 9 indeholder særlige regler om tavshedspligt, videregivelse og indhentning af helbredsoplysninger m.v.

Desuden kan de særlige kategorier af oplysninger behandles, hvis dette er nødvendigt af hensyn til en offentlig myndigheds varetagelse af sine opgaver på det strafferetlige område, jf. lovens § 7, stk. 6.

Endelig giver persondatalovens § 7, stk. 7, mulighed for, at tilsynsmyndigheden kan meddele tilladelse til behandling af de særlige kategorier af oplysninger, der er omfattet af § 7, af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser. Det overlades til tilsynsmyndigheden at fastsætte nærmere vilkår for behandlingen.

2.3.3.2. Databeskyttelsesforordningen

Følsomme oplysninger, der reguleres i forordningens artikel 9, må som udgangspunkt ikke behandles, på samme måde som i persondatalovens § 7 og databeskyttelsesdirektivets artikel 8. Det drejer sig om 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.

Afgræsning af, hvad der er følsomme personoplysninger svarer nogenlunde til den gældende retstilstand, dog er særligt ”biometriske data med det

formål entydigt at identificere en fysisk person” nu – i modsætning til retstilstanden efter persondataloven – en følsom personoplysning.

De følsomme oplysninger omfattet af artikel 9, stk. 1, må dog behandles, hvis der er hjemmel til det i forordningen, hvilket særligt vil sige i artikel 9, stk. 2, litra a-j. Behandling af de pågældende oplysninger kan således ske på betingelse af, at den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger (litra a), at 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 (litra b), at 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 (litra c), at 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 (litra d), at behandling vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede (litra e), at behandling er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol (litra f), at 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 (litra g), at behandling er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson og underlagt de betingelser og garantier, der er omhandlet i artikel 9, stk. 3 (litra h), at behandling er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet (litra i), eller at behandling er nødvendig til arkivformål i samfundets interesse, til

videnskabelige eller historiske forskningsformål eller til statistiske formål 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 (litra j).

Databeskyttelsesforordningens artikel 9, stk. 2, litra a, c, d, e og f, kan efter deres ordlyd anvendes som direkte behandlingshjemler, så længe behandlingsbetingelserne i de pågældende bestemmelser er opfyldt, f.eks. hvis behandlingen sker af hensyn til ”den registreredes eller en anden fysisk persons vitale interesser”, jf. artikel 9, stk. 2, litra c, jf. *betænkningen*, side 208 f. De pågældende bestemmelser i artikel 9, stk. 2, forudsætter således ikke en national, implementerende hjemmelslovgivning om selve den konkrete behandling af personoplysning – forordningens bestemmelser kan anvendes direkte som behandlingshjemmel.

Heroverfor synes artikel 9, stk. 2, litra b, g, h, i og j med henvisninger – dog med forskellig formulering – til EU-retten eller medlemsstaternes nationale ret, at forudsætte, at behandlingen er forankret i f.eks. national ret for, at udgangspunktet i artikel 9, stk. 1, om forbud mod behandling af følsomme oplysninger, kan fraviges. Det fremgår om disse litraer i præambelbetragtning nr. 52, 1. pkt., at ”[d]er bør også gives mulighed for at fravige forbuddet mod at behandle særlige kategorier af personoplysninger, når det er fastsat i EU-retten eller medlemsstaternes nationale ret og er omfattet af de fornødne garantier”.

Databeskyttelsesforordningens artikel 9, stk. 2, litra b, g, h, i og j, kræver således en udfyldning i EU-retten eller national ret og vil ikke uden videre kunne anvendes som direkte behandlingshjemmel.

Artikel 9, stk. 2, litra b, g, h, i og j, skal på den baggrund anses for både at være udtryk for et nationalt råderum til at vedtage regler om behandling af personoplysninger på de pågældende litraers områder, men også således, at de pågældende regler skal ”aktiveres” i national ret (eller i andre EU-retsakter) for, at forbuddet i artikel 9, stk. 1, kan anses for fraveget.

Artikel 9, stk. 2, litra h, kan aktiveres ”i henhold til en kontrakt med en sundhedsperson”, jf. bestemmelsens ordlyd. Det må i den forbindelse antages, at der ikke er noget til hinder for, at forordningens artikel 9, stk. 2, litra b, g, h, i og j, gennemføres som behandlingsregler på generel vis ved

en nærmest ordret implementering – på samme måde som med f.eks. persondatalovens § 7, stk. 7, der er en tekstnær implementering af databeskyttelsesdirektivets artikel 8, stk. 4.

Artikel 9, stk. 2, litra b, g, h, i og j, kan også aktiveres via national særlovgivning. Det må i den forbindelse antages at være tilstrækkeligt, at den pågældende behandling af personoplysninger er forudsat i særlovgivningen. Det kan således ikke være et krav, at den pågældende særlovgivning indeholder en udtrykkelig regel om behandlingen af personoplysninger i forbindelse med brug af f.eks. artikel 9, stk. 2, litra g, om ”væsentlige samfundsinteresser”.

Formuleringen af artikel 9, stk. 2, litra b, g, h, i og j, må i den forbindelse også forstås således, at man nationalt kan beslutte alene at aktivere de forskellige litraer som hjemmelsgrundlag i et vist omfang. Eksempelvis omhandler artikel 9, stk. 2, litra b, ”arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder”. I og med at litra b, g, h, i og j ikke kan anvendes uden videre som direkte behandlingsgrundlag må medlemsstaterne lovgivningsmæssig kunne bestemme, at alene en del heraf skal kunne anvendes – i litra b’s tilfælde, f.eks. alene for så vidt angår ”arbejdsretlige forpligtelser”. I det omfang medlemsstaterne ikke har valgt at aktivere hele eller dele af de pågældende bestemmelser i sin lovgivning, falder man tilbage på forbuddet i artikel 9, stk. 1, mod at behandle de pågældende følsomme personoplysninger.

Der henvises i den forbindelse til *betænkningen*, side 223-227.

2.3.3.3. Justitsministeriets overvejelser og lovforslagets udformning

Det er Justitsministeriets vurdering, at der i meget vidt omfang efter databeskyttelsesforordningens artikel 9, stk. 2, litra a, c, d, e og f vil kunne behandles *følsomme oplysninger* i samme omfang, som det er tilfælde i dag efter persondatalovens § 7, stk. 2 og 4. Der henvises også her til det ovenfor anførte om mulighederne for at behandle oplysninger efter forordningens artikel 9.

Som nævnt ovenfor nødvendiggør forordningens artikel 9, stk. 2, litra b, g, h, i og j, at behandlingen er forankret i f.eks. national ret for, at udgangspunktet i artikel 9, stk. 1, om forbud mod behandling af følsomme oplysninger, kan fraviges.

Efter Justitsministeriets opfattelse bør vurderingen af, i hvilken grad de pågældende muligheder for at fravige udgangspunktet om forbud mod behandling af følsomme oplysninger, skal ”aktiveres” styres en tanke om, at det skal være muligt at behandle følsomme oplysninger i samme omfang som i efter den nugældende persondatalov.

Det er på den baggrund Justitsministeriets vurdering, at der skal fastsættes regler om mulighed for nødvendig behandling til overholdelse den dataansvarliges eller den registreredes arbejdsretlige forpligtelser og specifikke rettigheder, med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt og af hensyn til væsentlige samfundsinteresse. Tilsynsmyndigheden giver tilladelse hertil, hvis behandlingen efter 1. pkt. ikke foretages af eller for en offentlig myndighed. Der kan i en tilladelse efter 2. pkt. fastsættes nærmere vilkår for behandlingen.

Det kan dog være vanskeligt på forhånd fuldstændigt at forudse behovet for at kunne behandle personoplysninger omfattet af forordningens artikel 9. Der foreslås derfor indført en bemyndigelse til, at vedkommende minister – efter forhandling med justitsministeren og inden for forordningens rammer – kan fastsætte yderligere regler om lovlig behandling af personoplysninger omfattet af forordningens artikel 9.

Som nævnt ovenfor nødvendiggør forordningens artikel 9, stk. 2, litra b, g, h, i og j, at behandlingen er forankret i f.eks. national ret for, at udgangspunktet i artikel 9, stk. 1, om forbud mod behandling af følsomme oplysninger, kan fraviges.

Det fremgår i øvrigt af databeskyttelsesforordningens artikel 9, stk. 2, litra b, g, h, i og j, at lovgiver – i forbindelse med udnyttelse af råderummet i de pågældende litraer – skal iagttage visse krav som nærmere beskrevet i bestemmelserne, eksempelvis skal der efter artikel 9, stk. 2, litra g, fastsættes passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder.

Sådanne krav om fastsættelse af passende og specifikke foranstaltninger bevirker, at det i forbindelse med udarbejdelse af den nationale lov skal vurderes, hvilke foranstaltninger der kan fastsættes udover de foranstaltninger, som allerede følger af forordningen. I den forbindelse kan det fast-

sættes, at den dataansvarlige pålægges pligten til at sikre passende og specifikke foranstaltninger. Endvidere er parterne i en overenskomst forpligtede til at iagttage de fornødne garantier, og parterne har således ansvaret herfor, når der fastsættes bestemmelser efter forordningens artikel 9, stk. 2, litra b.

Med dette lovforslag er det hensigten at pålægge den dataansvarlige pligten til at sikre passende og specifikke foranstaltninger i den omfang lovforslagets § 7 aktiverer behandlingsmulighederne i forordningens artikel 9, stk. 2, litra b, g, h, i og j. Der henvises i den forbindelse til *betænkningen*, side 225-226.

Det betyder i bund og grund, at den dataansvarlige skal sikre, at personoplysninger behandles i overensstemmelse med databeskyttelsesforordningen.

I *betænkningen*, side 225-226, nævnes – som inspiration til, hvad der kan være passende og specifikke foranstaltninger – hvad Registerudvalget i betænkning nr. 1345 fandt, var *tilstrækkelige garantier*. Registerudvalget anførte således i betænkning nr. 1345/1997 om behandling af personoplysninger, side 252, at der var tale om tilstrækkelige garantier i forbindelse med indførelsen af persondatalovens § 9, vedtaget indenfor rammerne af databeskyttelsesdirektivets artikel 8, stk. 4, om retsinformationssystemer, når det blev indført, at tilsynsmyndigheden kunne fastsætte nærmere vilkår for behandlinger, og når der blev stillet vilkår om, at personnavne, præcise adresseangivelser og eventuelt andre identifikationsoplysninger fjernes, herunder vilkår om, at der ikke måtte kunne søges på navne mv., i det omfang der ikke skete anonymisering. Særligt i forbindelse med retsinformationssystemer fandt Registerudvalget, at der var tale om tilstrækkelige garantier, når det i loven blev fastsat, at oplysninger, som behandledes ikke senere måtte behandles i andet øjemed

Som en del af den dataansvarliges ”værktøjskasse” – med henblik på at sikre, at lovforslaget og databeskyttelsesforordningen overholdes, herunder de grundlæggende principper i artikel 5 og krav til behandlingssikkerhed i artikel 32, ved behandling af følsomme personoplysninger omfattet af artikel 9 – kan *eksempelvis* følgende foranstaltninger også nævnes:

- Tekniske og organisatoriske foranstaltninger til sikring af, at behandlingen er i overensstemmelse med forordning

- Foranstaltninger til sikring af, at det er muligt efterfølgende at undersøge og fastslå, om og af hvem der er behandlet personoplysninger (logning)
- Frivillig udpegning af databeskyttelsesrådgiver, jf. databeskyttelsesforordningens artikel 37, stk. 4
- Fastsættelse af interne regler om organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer.
- Foranstaltninger til sikring af, at alene personer, som den dataansvarlige autoriserer hertil, fordi det er nødvendigt, kan få adgang til personoplysninger
- Fastsættes af retningslinjer for den dataansvarliges tilsyn med overholdelsen af de sikkerhedsforanstaltninger, herunder løbende opfølgning og revision
- Fornøden instruktion fra den dataansvarliges side til de medarbejdere, som behandler personoplysningerne.
- Foranstaltninger – på steder, hvor der foretages behandling af personoplysninger – henblik på at forhindre uvedkommendes adgang til oplysningerne.
- Pseudonymisering af personoplysninger
- Kryptering af personoplysninger
- Sikring af vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester i forbindelse med behandling af personoplysninger
- Sikring af sikkerheden i behandlingen, etablering af mekanismer for regelmæssig revision, vurdering og evaluering af effektiviteten af tekniske og organisatoriske foranstaltninger
- Registrering af afviste adgangsforsøg og tekniske foranstaltninger, der kan sikre blokering for yderligere forsøg, hvis det er nødvendigt

Der kan i den forbindelse søges inspiration i den hidtidige gældende sikkerhedsbekendtgørelse, bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001.

Der henvises til bemærkningerne til lovforslagets § 7.

2.3.4. Behandling af oplysninger om strafbare forhold

2.3.4.1. Gældende ret

I persondatalovens § 8 er der fastsat betingelser for, hvornår offentlige og private kan behandle oplysninger om strafbare forhold. Persondatalovens § 8, stk. 1-3 omhandler, hvornår offentlige myndigheder kan behandle og videregive oplysninger om bl.a. strafbare forhold.

Det følger således af § 8, stk. 1, at der for den offentlige forvaltning ikke må behandles oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver. Det følger af § 8, stk. 2, at de i stk. 1 nævnte oplysninger må ikke videregives. Videregivelse kan dog ske, hvis 1) den registrerede har givet sit udtrykkelige samtykke til videregivelsen, 2) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår, 3) videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe, eller 4) videregivelsen er nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige. Det følger af § 8, stk. 3, at forvaltningsmyndigheder, der udfører opgaver inden for det sociale område, kun må videregive de i stk. 1 nævnte oplysninger og de oplysninger, der er nævnt i § 7, stk. 1, hvis betingelserne i stk. 2, nr. 1 eller 2, er opfyldt, eller hvis videregivelsen er et nødvendigt led i sagens behandling eller nødvendig for, at en myndighed kan gennemføre tilsyns- eller kontrolopgaver.

Det fremgår af persondatalovens § 8, stk. 4 og 5, at private dataansvarlige – efter snævre betingelser – bl.a. kan behandle og videregive oplysninger om strafbare forhold.

Det følger således af § 8, stk. 4, at private må behandle oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Herudover kan behandling ske, hvis det er nødvendigt til varetagelse af en berettiget interesse og denne interesse klart overstiger hensynet til den registrerede. Det følger af § 8, stk. 5, at de i stk. 4 nævnte oplysninger ikke må videregives uden den registreredes udtrykkelige samtykke. Videregivelse kan dog ske uden samtykke, når det sker til varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse.

2.3.4.2. Databeskyttelsesforordningen

Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger er reguleret i forordningens artikel 10. Det fremgår af artikel 10, 1. pkt., at behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på grundlag af forordningens artikel 6, stk. 1, kun må foretages under kontrol af en offentlig myndighed, eller hvis behandlingen har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for de registreredes rettigheder og frihedsrettigheder.

Det bemærkes, at betegnelsen i forordningens artikel 10 om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger er lig udtrykket ”strafbare forhold”, der følger af gældende ret. Der henvises til *betænkningen*, side 244.

For så vidt angår offentlige myndigheder, følger det af artikel 10, 1. pkt., at behandlingsgrundlaget for oplysninger om strafbare forhold er forordningens artikel 6, stk. 1, om almindelige personoplysninger. Det betyder, at oplysninger om strafbare forhold – efter forordningen – skal anses for almindelige personoplysninger, og således ikke omfattet af de særlige behandlingsregler for følsomme oplysninger i forordningens artikel 9.

Det må antages, at det er muligt at videreføre de særlige regler i gældende ret for offentlige myndigheders behandling og videregivelse af oplysninger om strafbare forhold efter persondatalovens § 8, stk. 1-3, på baggrund af forordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2 og 3.

Private kan efter forordningens artikel 10, 1. pkt., sidste led, alene behandle oplysninger om strafbare forhold, hvis behandlingen har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder.

Det kan derfor antages, at de ”snævre betingelser” for privates behandling af oplysninger om strafbare forhold efter gældende ret vil kunne videreføres inden for rammerne af forordningens artikel 10, 1. pkt., idet en sådan begrænsning må antages at udgøre passende garantier for den registreredes rettigheder og frihedsrettigheder.

For at private kan behandle oplysninger om straffbare forhold, skal der således fastsættes nationale regler herom, som giver passende garantier for registreredes rettigheder og frihedsrettigheder.

Der henvises til *betænkningen* side 243-248.

2.3.4.3. Justitsministeriets overvejelser og lovforslagets udformning

For så vidt angår den nuværende regulering efter persondatalovens § 8 er det Justitsministeriet vurdering, at bestemmelsen skal opretholdes også i fremtiden for så vidt angår behandling af oplysninger om straffbare forhold.

Det må antages, at det er muligt at fastsætte regler svarende til de særlige regler i gældende ret for offentlige myndigheders behandling og videregivelse af oplysninger om straffbare forhold efter persondatalovens § 8, stk. 1-3, på baggrund af forordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2 og 3.

Dette skal ses på baggrund af, at Justitsministeriet vurderer, at der også fremover er et særligt beskyttelseshensyn i forhold til behandling af oplysninger om straffbare forhold.

For så vidt angår privates mulighed for at behandle oplysninger om straffbare forhold, er det Justitsministeriets vurdering, at de snævre betingelser for, hvornår private kan behandle oplysninger om straffbare forhold efter persondatalovens §§ 8, stk. 4 og 5, må antages at udgøre *specifikke og tilstrækkelige garantier* i overensstemmelse kravet til nationale regler i forordningens artikel 10, 1. pkt., sidste led. På denne baggrund foreslår Justitsministeriet, at der i lovforslaget skabes sammen behandlingsmuligheder for private for så vidt angår straffbare forhold som efter persondatalovens §§ 8, stk. 4 og 5.

For så vidt angår den del af persondatalovens § 8, der vedrører behandling af oplysninger om væsentlige sociale problemer og andre rent private forhold henvises til beskrivelsen ovenfor under afsnittet om almindelige oplysninger.

2.3.5. Behandling af oplysninger i forbindelse med retsinformationssystemer

2.3.5.1. Gældende ret

Ved behandling af personoplysninger i forbindelse med førelse af et retsinformationssystem skal de grundlæggende behandlingsprincipper i person-

datalovens § 5 og behandlingsbetingelserne i lovens §§ 6 og 9 iagttages.

Ikke-følsomme personoplysninger kan bl.a. behandles, hvis det er nødvendigt af hensyn til udførelsen af en opgave i samfundets interesse, jf. lovens § 6, stk. 1, nr. 5.

Ifølge persondatalovens § 9, stk. 1, kan oplysninger omfattet af §§ 7 og 8 – som ellers ikke vil kunne behandles – behandles med henblik på at føre retsinformationssystemer af væsentlige samfundsmæssige betydning, hvis behandlingen er nødvendig for førelsen af systemerne.

Efter § 9, stk. 2, må sådanne oplysninger ikke senere behandles i andet øjemed. Det samme gælder for behandlinger af ikke-følsomme oplysninger, som alene foretages med henblik på at føre retsinformationssystemer. Endvidere følger det af § 9, stk. 3, at tilsynsmyndigheden kan meddele nærmere vilkår for de i stk. 1 nævnte behandlinger. Tilsvarende gælder for de i § 6 nævnte oplysninger, som alene behandles i forbindelse med førelsen af retsinformationssystemer.

Af bemærkningerne til persondatalovens § 9 fremgår det bl.a., at nødvendighedskravet i stk. 1 betyder, at bestemmelsen ikke hjemler adgang til at behandle oplysninger i et retsinformationssystem, hvis systemet kunne tjene sit formål ligeså sikkert og effektivt uden oplysninger om enkeltpersoner. Det fremgår endvidere, at bestemmelsen i stk. 2 indebærer, at oplysningerne ikke må anvendes til at træffe foranstaltninger eller afgørelser vedrørende registrerede personer, og at dette gælder behandling af både følsomme oplysninger og ikke-følsomme oplysninger, som i henhold til §§ 6 og 9 alene foretages med henblik på at føre retsinformationssystemer. Desuden fremgår det, at oplysningerne naturligvis må anvendes i forbindelse med f.eks. førelse af en retssag, idet en sådan anvendelse ikke ligger uden for formålet med et retsinformationssystem. Om stk. 3 fremgår det, at bestemmelsen sikrer, at der kan fastsættes vilkår for behandling af følsomme oplysninger og nærmere vilkår for ikke-følsomme oplysninger, som alene sker i tilknytning til førelsen af retsinformationssystemer. Der kan f.eks. fastsættes vilkår om, at personnavne, præcise adresseangivelser og eventuelt andre identifikationsoplysninger fjernes i samme omfang, som dette skal ske efter Justitsministeriets cirkulære nr. 85 af 8. juli 1988 om indlæggelse af afgørelser i Retsinformation. Det fremgår af Registerudvalgets betænkning 305, at retsinformationssystemer, som ikke var reguleret af registerlovene, skulle være reguleret af persondataloven, i det omfang de indeholdt personoplysninger, som konsekvens af databaseskyttelsesdirek-

tivet. Desuden fremgår det, at bestemmelsen i § 9, stk. 1, er indsat på baggrund af artikel 8, stk. 4, ifølge hvilken der af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, kan fastsættes undtagelser fra artikel 8, stk. 1, om forbud mod behandling af følsomme oplysninger (gennemført ved persondatalovens § 7, stk. 1), såfremt der gives tilstrækkelige garantier. Endelig fremgår det, at der med indsættelsen af bestemmelserne i persondatalovens § 9, stk. 3, hvorefter tilsynsmyndigheden kan fastsætte nærmere vilkår for behandlinger, der alene finder sted med henblik på at føre retsinformationssystemer, etableres tilstrækkelige garantier, og at der yderligere bidrages til etableringen heraf ved fastsættelsen af begrænsningen af behandling af oplysninger i § 9, stk. 2.

Der henvises til *betænkning* side 256-259.

2.3.5.2. Databeskyttelsesforordningen

Databeskyttelsesforordningen indeholder regler, som i vidt omfang svarer til reglerne i databeskyttelsesdirektivets artikel 5 og 8, stk. 4, og som dermed må antages på samme måde som i dag at give medlemsstaterne mulighed for at fastsætte nærmere regler under forudsætning af, at der gives tilstrækkelige garantier, der præciserer reglerne i forordningen.

Det må derfor antages, at det er muligt at videreføre en bestemmelse svarende til persondatalovens § 9, når forordningen får virkning 25. maj 2018.

Der henvises til *betænkningen* side 259-261.

2.3.5.3. Justitsministeriets overvejelser og lovforslagets udformning

Retsinformationssystemer vil i mange tilfælde indeholde personoplysninger, herunder også oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold og oplysninger om helbredsforhold og seksuelle forhold. Justitsministeriet finder det derfor hensigtsmæssigt, at der indsættes en udtrykkelig bestemmelse i lovgivningen, hvorefter de nævnte særlige kategorier af oplysninger samt oplysninger om strafbare forhold kan behandles, såfremt dette alene sker med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning, og behandlingen er nødvendig for førelsen af systemerne.

Herudover foreslås det, at oplysninger, som indgår i et retsinformationssystem, ikke senere må behandles i andet øjemed. Udvalget er af den opfat-

telse, at den udtrykkelige begrænsning i den videre behandling af oplysningerne bidrager til etableringen af tilstrækkelige garantier mod misbrug af oplysninger i retsinformationssystemer. Udvalgets forslag om, at tilsynsmyndigheden skal kunne meddele vilkår for behandlingen af oplysninger i retsinformationssystemer, skal også ses som en garanti mod misbrug.

Der henvises til lovforslaget § 9.

2.3.6. Behandling af oplysninger i statistik eller videnskabeligt øjemed

2.3.6.1. Gældende ret

I persondatalovens § 10 fastsættes særlige regler for behandling i statistisk eller videnskabeligt øjemed. Bestemmelsen har sin baggrund i direktivets artikel 8, stk. 4, hvorefter medlemsstaterne af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, kan fastsætte andre undtagelser fra behandlingsforbuddet i artikel 8, stk. 1, end dem, som følger af artikel 8, stk. 2 og 3.

Efter bestemmelsen i *stk. 1* vil der kunne behandles oplysninger som nævnt i § 7, stk. 1, eller § 8, såfremt behandlingen alene finder sted med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning.

Det følger af *stk. 2*, at der ikke senere må ske behandling af oplysninger, som er omfattet af stk. 1, til andre formål. Tilsvarende gælder med hensyn til behandling af andre oplysninger, som i henhold til § 6 alene foretages med henblik på at udføre statistiske eller videnskabelige undersøgelser.

Bestemmelsen i *stk. 3* fastsætter endelig, at videregivelse til tredjemand kun kan ske efter forudgående tilladelse fra vedkommende tilsynsmyndighed og i givet fald kun med henblik på udførelse af undersøgelser i statistisk eller videnskabeligt øjemed, jf. stk. 1 og 2. Efter bestemmelsen kan vedkommende tilsynsmyndighed meddele vilkår til sikring af, at oplysningerne alene vil blive anvendt til statistiske eller videnskabelige formål samt vilkår til beskyttelse af de registreredes privatliv.

Der henvises til *betænkningen* side 102-107.

2.3.6.2. Databeskyttelsesforordningen

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.

Forordningens artikel 9, stk. 2, litra j, om behandling af oplysninger 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.

Medlemsstaterne har således mulighed for at fastsætte 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.

Der henvises til betænkningen side 107-113 og side 981-990.

2.3.6.3. Justitsministeriets overvejelser og lovforslagets udformning

Det er Justitsministeriets vurdering, at der skal opretholdes regler, der svarer til persondatalovens § 10 om behandling af personoplysninger med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for udførelsen af undersøgelserne.

Justitsministeriet har herved lagt vægt på, at den nugældende § 10 skaber en fornuftig balance mellem hensynet til forskning og statistik og hensynet til beskyttelsen af personoplysninger.

Justitsministeriet skal hertil bemærke, at det er ministeriets vurdering, at en national regel svarende til den nuværende persondatalovs § 10, kan fastsættes inden for rammerne af forordningens artikel 89, stk. 1 og artikel 9, stk. 2, litra j.

Herudover er det Justitsministeriets vurdering, at der som noget nyt i forhold til persondatalovens § 10, inden for rammerne af forordningen, skal gives mulighed for en videre behandling til andre formål end videnskabelige eller historiske forskningsformål på baggrund af samtykke fra den registrerede eller ved særlige omstændigheder, herunder hensynet til den registreredes (vitale) interesser. Der henvises til lovforslagets § 10.

2.3.7. Behandling af oplysninger om personnummer

2.3.7.1. Gældende ret

Det følger af persondatalovens § 11, stk. 1, at offentlige myndigheder vil kunne behandle oplysninger om personnumre med henblik på en entydig identifikation samt som journalnummer.

I persondatalovens § 11, stk. 2, fastsættes regler for privates behandling af oplysninger om personnumre.

Efter reglen i *nr. 1* vil private virksomheder m.v. kunne foretage behandling, herunder registrering og videregivelse, af oplysninger om personnumre, såfremt det følger af lov eller bestemmelser fastsat i henhold til lov.

Herudover vil der efter bestemmelsen kunne ske behandling af oplysninger om personnumre, hvis den registrerede har givet sit udtrykkelige samtykke hertil, jf. *nr. 2*. Et sådant samtykke skal opfylde betingelserne i § 3, nr. 8.

Endelig vil der efter bestemmelsen *nr. 3* kunne ske behandling uden samtykke, hvis dette alene sker i forbindelse med undersøgelser i videnskabeligt eller statistisk øjemed.

Af bestemmelsen i persondatalovens § 11, stk. 3, følger, at private dataansvarliges behandling af oplysninger om personnumre i henhold til bestemmelsen i stk. 2, nr. 3, ikke må indebære, at der sker offentliggørelse af oplysningerne uden den registreredes udtrykkelige samtykke.

Der henvises til betænkningen side 966-968.

2.3.7.2. Databeskyttelsesforordningen

Oplysninger om personnumre er almindelige oplysninger omfattet af forordningens artikel 6. Dog fremgår det af databeskyttelsesforordningens artikel 87, 1. pkt., at medlemsstaterne nærmere kan fastsætte de specifikke betingelser for behandling af et nationalt identifikationsnummer eller andre almene 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 fornødne garantier for den registreredes rettigheder og frihedsrettigheder i henhold til forordningen. 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.

Der henvises til *betænkningen* side 986-969.

2.3.7.3. Justitsministeriets overvejelser og lovforslagets udformning

Det er Justitsministeriets vurdering, at persondatalovens regulering af behandling af oplysninger om personnumre også bør fortsættes. Det er således Justitsministeriet vurdering, at der fortsat bør gælde særlige betingelser for behandling af oplysninger om personnumre. Det er endvidere Justitsministeriets vurdering, at betingelserne for behandling af oplysninger om personnumre i lovforslaget respekterer 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.

Justitsministeriet finder dog, at private – i modsætning til i dag – bør have mulighed for at behandle oplysninger om personnumre, når betingelserne i forslaget § 7 er opfyldt. Der kan i den forbindelse bl.a. henvises til, at der stilles skærpede krav til behandlingsgrundlag i forslaget § 7 om følsomme oplysninger. I tilfælde, hvor de skærpede betingelser for at behandle følsomme oplysninger er opfyldt vil der derfor være formodning for, at hensynet til integritet mv. er tilstrækkeligt varetaget også i relation til behandling af oplysninger om personnummer.

Der henvises til lovforslagets § 11.

2.3.8. Behandling af oplysninger i forbindelse med ansættelsesforhold

2.3.8.1. Gældende ret

Behandling af oplysninger i ansættelsesforhold sker i dag først og fremmest på baggrund af behandlingshjemlerne i persondatalovens §§ 6-8, jf. *betænkningen*, særligt side 118, og 970-976, om gældende ret i den forbindelse.

2.3.8.2. Databeskyttelsesforordningen

Det fremgår af forordningens artikel 88, stk. 1, at medlemsstaterne ved lov eller i medfør af kollektive overenskomster kan fastsætte mere specifikke bestemmelser for at sikre beskyttelse af rettighederne og frihedsrettighederne i forbindelse med behandling af 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 (lov)bestemmelser, som den vedtager i henhold til stk. 1, og underretter den straks om alle senere ændringer, der berører dem.

Både artikel 6, stk. 2-3 og artikel 9, stk. 2, efterlader muligheder for at fastsætte nærmere nationale regler om behandling af personoplysninger. 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.

Der henvises til *betænkningen* side 130 og 976-980.

2.3.8.3. Justitsministeriets overvejelser og lovforslagets udformning

Kollektive overenskomster og aftaler samt det fagretlige konfliktløsnings-system udgør en helt central, retligt bindende ramme for organiseringen af det danske arbejdsmarked. Kollektive overenskomster er også på europæisk plan anerkendt for sin særlige status i EU's charter for grundlæggende rettigheder. I chartret anerkender man således i artikel 28 arbejdsmarkedets parter forhandlingsret og ret til kollektive skridt. Samtidigt ligger det fast, at EU-direktiver kan gennemføres via kollektive overenskomster for lønmodtagergrupper, der er omfattet af overenskomsten.

Kollektive overenskomster kan på den baggrund muligvis statuere en "retlig forpligtelse" i den forstand, hvori udtrykket databeskyttelsesretligt er anvendt i forordningens artikel 6, stk. 1, litra c. Der henvises til *betænkningen*, side 118, 130 og 971.

Der er dog en vis usikkerhed forbundet med spørgsmålet, om en "retlig forpligtelse" i en *databeskyttelsesretligt* sammenhæng kan statueres i en kollektiv overenskomst. Herudover kan arbejdsgivere i det offentlige, i modsætning til i det private, ikke længere efter den 25. maj 2018, hvorfra forordningens skal anvendes, benytte sig af "interesseafvejningsreglen" i forordningens artikel 6, stk. 1, litra f, der fremover alene gælder for private. Den tilsvarende behandlingshjemmel i persondatalovens § 6, stk. 1, nr. 7, har hidtil været anvendt i vidt omfang som behandlingshjemmel af både offentlige og private arbejdsgivere.

I lyset af ovenstående og med henblik på som "helgardering" at sikre et solidt juridisk grundlag for behandling af personoplysninger på hele det danske arbejdsmarked også fremadrettet, foreslås der med lovforslagets § 12 indført en supplerende hjemmelsbestemmelse, hvorefter der også kan behandles personoplysninger på baggrund af kollektive overenskomster, både hvor overenskomsten foreskriver en *pligt* til behandlingen – f.eks. en pligt til at underrette tillidsrepræsentanten eller den faglige organisation ved afskedigelser – og hvor overenskomsten giver *mulighed* for eller *forudsætter* behandling af personoplysninger, f.eks. hvis overenskomsten giver arbejdsgiveren mulighed for under nærmere omstændigheder at overvåge medarbejderes brug af internettet eller at afkræve dem en urinprøve, eller hvis overenskomsten forudsætter videregivelse af personoplysninger til tillidsrepræsentanten eller den faglige organisation som led i lønforhandlinger eller fagretlig konfliktløsning mv.

Den foreslåede bestemmelse sikrer, at behandling af personoplysninger kan ske uafhængigt af, om den registrerede er medlem af en fagforening,

så længe den registreredes ansættelsesforhold er omfattet af den pågældende overenskomst.

Den foreslåede bestemmelse har sin baggrund i forordningens artikel 88, der giver medlemsstaterne mulighed at vedtage specifikke bestemmelser om behandling af arbejdstageres personoplysninger i ansættelsesforhold. Artikel 88 er 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. Der henvises til *betænkningen*, s. 970-980 om forordningens artikel 88.

Den foreslåede § 12 ændrer naturligvis ikke ved retstilstanden i dag om, at kollektive overenskomster skal ligge inden for den øvrige lovgivnings rammer. De kollektive overenskomster, der danner baggrund for behandling efter lovforslagets § 12, skal i øvrigt skal leve op til kravene hertil efter artikel 88, stk. 2.

Der henvises i øvrigt til bemærkningerne til lovforslagets § 12.

2.3.9. Behandling i forbindelse med markedsføring mv.

2.3.9.1. Gældende ret

I persondatalovens § 6, stk. 2-4, er der fastsat nærmere betingelser for behandling af personoplysninger i forbindelse med markedsføring.

Efter bestemmelsen i stk. 2, må en virksomhed ikke videregive oplysninger om en forbruger til en anden virksomhed til brug ved markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed, medmindre forbrugeren har givet sit udtrykkelige samtykke hertil.

Et samtykke skal indhentes i overensstemmelse med reglerne i markedsføringslovens § 10.

Efter bestemmelsen i stk. 3, kan videregivelse og anvendelse som nævnt i stk. 2 dog finde sted uden samtykke, hvis der er tale om generelle kundeoplysninger, der danner grundlag for inddeling i kundekategorier, og hvis betingelserne i persondatalovens § 6, stk. 1, nr. 7, er opfyldt.

Det følger af bestemmelsen i stk. 4, at der efter stk. 3 ikke må videregives eller anvendes oplysninger om omfattet af persondatalovens § 7, stk. 1, og

§ 8. Endvidere følger det af bestemmelsen, at justitsministeren kan fastsætte yderligere begrænsninger i adgangen til at videregive eller anvende bestemte typer af oplysninger efter stk. 3.

I persondatalovens § 12 er der fastsat regler om adresserings- og kuverteringsbureauer.

Det følger af § 12, stk. 1, at dataansvarlige, der med henblik på markedsføring sælger fortegnelser over grupper af personer, eller som for tredjemand foretager adressering eller udsendelse af meddelelser til sådanne grupper, kun må behandle 1) oplysninger om navn, adresse, stilling, erhverv, e-postadresse, telefon- og telefaxnummer, 2) oplysninger, der indgår i erhvervsregistre, som i henhold til lov eller bestemmelser fastsat i henhold til lov er beregnet til at informere offentligheden, samt 3) andre oplysninger, hvis den registrerede har givet udtrykkeligt samtykke dertil.

Et samtykke skal indhentes i overensstemmelse med markedsføringslovens § 10.

Det følger af § 12, stk. 2, at behandling af oplysninger som nævnt i stk. 1 dog ikke må omfatte oplysninger som nævnt i lovens § 7, stk. 1, og § 8. Endvidere følger det af bestemmelsen, at justitsministeren kan fastsætte yderligere begrænsninger i adgangen til at behandle bestemte typer af oplysninger.

2.3.9.2. Databeskyttelsesforordningen

Det fremgår af databeskyttelsesforordningens artikel 6, stk. 2, at medlemsstaterne *kan* opretholde eller indføre mere specifikke bestemmelser for at tilpasse anvendelsen af forordningens bestemmelser om behandling med henblik på overholdelse af stk. 1, litra c og e, ved at fastsætte mere præcist specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling, *herunder* for andre specifikke databehandlingssituationer som omhandlet i kapitel IX (artikel 85-91).

Det følger af databeskyttelsesforordningens artikel 6, stk. 3, der synes at fastsætte nærmere betingelser for at anvende artikel 6, stk. 2, at grundlaget for behandling i henhold til stk. 1, litra c og e, skal fremgå af EU-retten eller af medlemsstaternes nationale ret, som den dataansvarlige er underlagt. Databeskyttelsesforordningens artikel 6, stk. 3, skal ses i forlængelse af artikel 6, stk. 2. Artikel 6, stk. 3, er således en uddybning af, hvordan de bestemmelser, som indføres efter artikel 6, stk. 2, hvorefter medlemsstater-

ne *kan* opretholde eller indføre specifikke regler, nærmere vil skulle udformes.

Efter databeskyttelsesforordningen er det således muligt at opretholde og indføre mere specifikke bestemmelser for at tilpasse anvendelsen i forbindelse med artikel 6, stk. 1, litra c og e, vedrørende behandling på baggrund af en retlig forpligtelse eller i samfundets interesse.

2.3.9.3. Justitsministeriets overvejelser og lovforslagets udformning

For så vidt angår persondatalovens behandlingsregler vedrørende markedsføring i lovens § 6, stk. 2-4, og § 12, er det Justitsministeriets vurdering, at også disse regler kan og bør opretholdes.

Det er Justitsministeriets vurdering, at den registreredes bør have afgørende indflydelse på, i hvilket omfang der behandles personoplysninger om den pågældende med henblik på markedsføring.

Der bør derfor i lovforslaget fastsættes snævre grænser for, i hvilke tilfælde en virksomhed – uden den enkelte forbrugers samtykke – må videregive oplysninger om en forbruger til andre virksomheder til brug for markedsføring, jf. lovforslagets § 13.

Der henvises i øvrigt til bemærkningerne lovforslagets § 13.

2.3.10. Overførsel til arkiv

2.3.10.1. Gældende ret

Persondatalovens § 14 regulerer spørgsmålet om arkivering. Efter bestemmelsen kan oplysninger, som er omfattet af loven, overføres til opbevaring på arkiv efter reglerne i arkivlovgivningen. Bestemmelsen indebærer, at der vil kunne ske arkivering af behandlede oplysninger i det omfang, dette følger af reglerne i arkivlovgivningen. Dette gælder for oplysninger, som er behandlet for såvel offentlige som for private.

Der henvises til *betænkningen* side 990-991.

2.3.10.2. Databeskyttelsesforordningen

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 endvidere 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.

I det omfang der fastsættes fornødne garantier 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 der således fastsættes nationale særregler herom.

Der henvises til *betænkningen* side 991-995.

2.3.10.3. Justitsministeriets overvejelser og lovforslagets udformning

I forhold til persondatalovens § 14, hvorefter oplysninger, der er omfattet af loven, kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen, lægges der med lovforslaget op til, at samme retstilstand fastsættes i lovforslaget.

Justitsministeriet lægger i den forbindelse vægt på, at der ved uformningen af bestemmelsen i forslaget skabes klarhed om reglerne om arkivering af personoplysninger mv.

Der henvises til lovforslagets § 14.

Afslutningsvis i dette afsnit om forordningens behandlingsregler finder Justitsministeriet anledning til at bemærke, at i det store omfang, at databeskyttelsesforordningen og dette lovforslag – herunder med bestemmelserne i § 7, der ”aktiverer” visse af hjemmelsgrundlagene i forordningens artikel 9, stk. 2, om følsomme oplysninger – viderefører samme muligheder for at behandle personoplysninger som efter den gældende retstilstand, må Datatilsynets hidtidige praksis om de pågældende hjemmelsgrundlag også efter den 25. maj 2018, hvorfra forordningen finder anvendelse, kunne anvendes som fortolkningsbidrag.

2.3.11. Kreditoplysningsområdet

2.3.11.1. Gældende ret

Den nærmere regulering af den virksomhed, der udøves af kreditoplysningsbureauer, og som består i at registrere og videregive oplysninger til bedømmelse af personers eller virksomheders økonomiske soliditet og kreditværdighed, er indeholdt i persondatalovens kapitel 5 og 6.

Persondatalovens kapitel 5 indeholder reglerne for den offentlige forvaltnings videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige. Reglerne har til formål at bidrage til en effektivisering af inddrivelsen af restancer til det offentlige gennem en større lighed gennem en større lighed i behandlingen af gæld til det offentlige og gæld til private, hvad angår mulighederne for at videregive oplysninger om gælden til kreditoplysningsbureauer. Denne lighed er dog ikke fuldstændig, idet der gælder en række yderligere garantier til beskyttelse af den registrerede, når videregivelsen foretages af en offentlig myndighed.

I persondatalovens kapitel 6 fastsættes detaljerede regler om kreditoplysningsbureauers virksomhed. Reglerne i persondatalovens kapitel 6 om kreditoplysningsbureauer har ikke sit direkte modstykke i databeskyttelsesdirektivet, men er vurderet at falde inden for de rammer, som direktivet giver for at fastsætte særlige regler om behandling af personoplysninger på nærmere bestemte områder. Reglerne i persondatalovens kapitel 6 gælder ikke alene for behandling af oplysninger om fysiske personer, men også for behandling af oplysninger om virksomheder mv., uanset om der er tale om en juridisk person.

Kreditoplysningsbureauernes virksomhed bygger ofte på et abonnements-system, der forudsætter en gensidig udveksling af oplysninger mellem kreditorer (abonnenterne) og bureauet. Abonnenterne får adgang til bureauets registreringssystem mod indgåelse af en abonnementsaftale. En sådan aftale indeholder endvidere i almindelighed en række vilkår for levering og anvendelse af oplysningerne.

Herudover registrerer bureauerne typisk af egen drift oplysninger indhentet fra Statstidende.

Der henvises til Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, side 63-65, 108-118 og 277-282.

2.3.11.2. Databeskyttelsesforordningen

Databeskyttelsesforordningen indeholder ikke en særregulering af kreditoplysningsområdet.

Det er derfor forordningens almindelige regler, der finder anvendelse på behandling af oplysninger inden for dette område, hvis der ikke vedtages danske særregler om kreditoplysningsbureauer.

Databeskyttelsesforordningen indeholder i kapitel III regler om den registreredes rettigheder, som den 25. maj 2018 finder anvendelse i stedet for reglerne i persondataloven.

Forordningens artikel 13 og 14 indeholder regler om oplysningspligt for den dataansvarlige.

Endvidere indeholder forordningens artikel 16, 17 og 18 regler om ret til berigtigelse, sletning og begrænsning af behandling.

Forordningens artikel 19 indeholder en underretningspligt i forbindelse med bl.a. berigtigelse, hvorefter den dataansvarlige underretter hver modtager, som personoplysningerne er videregivet til, om enhver berigtigelse eller sletning af personoplysningerne eller begrænsning af behandling, der er udført i henhold til artikel 16, artikel 17, stk. 1, og artikel 18, medmindre dette viser sig umuligt eller er uforholdsmæssigt vanskeligt. Den dataansvarlige oplyser den registrerede om disse modtagere, hvis den registrerede anmoder herom. For nærmere herom se herved *betænkningen*, side 342-346.

2.3.11.3. Justitsministeriets overvejelser og lovforslagets udformning

Databeskyttelsesforordningen giver mulighed for, at der i vidt omfang kan fastsættes særlige regler om behandling af oplysninger, jf. herved også *betænkningen*, side 161 ff.

Det er af meget væsentlig betydning for såvel enkeltpersoner som virksomheder, at behandling af oplysninger i kreditoplysningsøjemed sker på en saglig og lovlig måde. Ulovlige behandlinger på dette område vil kunne medføre meget alvorlige skadevirkninger for de involverede parter.

Der bør derfor efter Justitsministeriets opfattelse også i den fremtidige lovgivning fastsættes særlige regler for sådan behandling af oplysninger.

Justitsministeriet vurderer, at bestemmelserne i persondatalovens § 15, § 16, § 17, § 18, § 19, § 20 og den del af § 23, der ikke vedrører den registrerede, kan opretholdes på grundlag af forordningens artikel 6, stk. 1, litra e, hvorefter behandling er lovlig, hvis den er nødvendig at hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, jf. artikel 6, stk. 2-3. Justitsministeriet vurderer således, at det er i samfundets interesse,

at der er særlige regler om kreditoplysningsbureauer, idet behandlinger på dette område som nævnt vil kunne medføre meget alvorlige skadevirkninger for de involverede parter.

Justitsministeriet vurderer endvidere, at bestemmelserne lever op til kravet i forordningens artikel 6, stk. 2, om at være mere *specifikke* bestemmelser om anvendelsen af forordningen. Reglerne er således specifikt afgrænset til at vedrøre særlige oplysninger i form af oplysninger om økonomisk soliditet og kreditværdighed, ligesom behandlingen foregår ved nærmere regulerede kreditoplysningsbureauer – og således vedrører et helt specifikt område for behandling.

Justitsministeriet vurderer dernæst, at det er nødvendigt med særlige behandlingsregler for personoplysninger ved kreditoplysningsbureauer, idet behandlinger på dette område som nævnt vil kunne medføre meget alvorlige skadevirkninger for de involverede parter. Det er således af væsentlig betydning for såvel enkeltpersoner som virksomheder, at behandling af oplysninger i kreditoplysningsøjemed sker på en saglig og lovlige måde.

Databeskyttelsesforordningen indeholder som nævnt i kapitel III reglerne om den registreredes rettigheder. Justitsministeriet foreslår derfor, at de regler i persondatalovens kapitel 5 og 6, som vedrører den registreredes rettigheder, ikke videreføres i lovforslaget. Det vil således være forordningens regler om den registreredes rettigheder, som fremover bør finde anvendelse på kreditoplysningsbureauers behandling af personoplysninger. Endvidere vil de særlige regler i lovforslaget om den registreredes rettigheder også finde anvendelse.

Forordningens artikel 12, 13 og 14 om oplysningspligt skal herefter anvendes i stedet for persondatalovens § 21, § 22 og den del af § 23, der vedrører den registrerede. Endvidere skal forordningens artikel 16, 17 og 18 om ret til berigtigelse, sletning og begrænsning af behandling anvendes i stedet for persondatalovens § 24 og § 26. Endelig skal forordningens artikel 19 om underretningspligt ved bl.a. berigtigelse anvendes i stedet for persondatalovens § 25.

Idet databeskyttelsesforordningens regler om de registreredes rettigheder nu erstatter de tidligere regler herom i persondataloven, vurderer Justitsministeriet – at virksomheder mv., der efter lovforslaget omfattes af forslaget, når behandlingen udføres for kreditoplysningsbureauer – også bør have rettigheder efter forordningens artikel 12-19. Justitsministeriet vurderer, at

denne ordning er hensigtsmæssig, så virksomheder mv. ligesom efter den gældende persondatalov, fortsat har rettigheder, når der behandles oplysninger for kreditoplysningsbureauer.

Justitsministeriet vurderer, at denne ordning er hensigtsmæssig og vurderer ikke, at en ophævelse af disse bestemmelser i persondataloven bevirker, at hensynet bag de særlige regler for kreditoplysningsbureauer ikke længere iagttages. Reglerne i forordningen om de registreredes rettigheder giver således den fornødne beskyttelse af den registrerede.

Justitsministeriet vurderer endelig, at det er hensigtsmæssigt, at tilladelsesordningen fra Datatilsynet skal opretholdes.

Det bemærkes, at i det omfang, spørgsmål om kreditoplysningsbureauers virksomhed ikke måtte være reguleret i kapitlerne, gælder lovforslaget og databeskyttelsesforordningens almindelige regler. Dette indebærer bl.a., at forordningens regler om de registreredes rettigheder om bl.a. oplysningspligt og retten til berigtigelse som nævnt finder anvendelse på kreditoplysningsbureauer.

2.4. Den registreredes rettigheder

2.4.1. Gældende ret

2.4.1.1. Persondatalovens § 28, stk. 1, og § 29, stk. 1, fastsætter regler om den dataansvarliges oplysningspligt over for den registrerede. Endvidere fastsætter persondatalovens kapitel 9 (§§ 31-34) reglerne om den registreredes indsigtret. Endelig fastsætter persondatalovens § 39, stk. 3, en ret til oplysning i forbindelse med automatiske afgørelser.

Persondatalovens § 30 indeholder regler om, i hvilke tilfælde oplysningspligten og indsigtretten kan begrænses, jf. også henvisninger hertil i lovens § 32, stk. 1, og § 39, stk. 3. Der henvises til *betænkningen*, side 389-396.

Det følger af lovens § 30, stk. 1, at bestemmelserne i § 28, stk. 1, og § 29, stk. 1, ikke gælder, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv.

Det følger endvidere af lovens § 30, stk. 2, at undtagelse fra bestemmelserne i § 28, stk. 1, og § 29, stk. 1, tillige kan gøres, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige interesser, herunder navnlig til statens sikkerhed, forsvaret, den offentlige sikkerhed, forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv, væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteinliggender, og kontrol-, tilsyns- eller reguleringsopgaver, herunder opgaver af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på nogle af de ovennævnte områder.

2.4.1.2. Det følger af persondatalovens § 32, stk. 2, at oplysninger, der behandles for den offentlige forvaltning som led i administrativ sagsbehandling, kan undtages fra indsichtsretten i samme omfang som efter reglerne i §§ 19-29 og 35 i lov om offentlighed i forvaltningen.

2.4.1.3. Det følger af persondatalovens § 32, stk. 3, at der ikke er ret til indsigt i oplysninger, der behandles for domstolene, hvis oplysningerne indgår i tekst, som ikke foreligger i endelig form. Dette gælder dog ikke, hvis oplysningerne er videregivet til en tredjemand. Der er ikke ret til indsigt i voteringsprotokoller og andre referater af domstolenes rådslagning samt materiale udarbejdet af domstolene til brug for rådslagningen.

2.4.1.4. Det følger af persondatalovens § 32, stk. 4, at indsichtsretten, jf. § 31, stk. 1, ikke finder anvendelse, hvis oplysningerne udelukkende behandles i videnskabeligt øjemed, eller hvor oplysningerne kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker.

2.4.1.5. Persondatalovens § 36 fastsætter regler om en forbrugers indsigelsesret over for virksomheders videregivelse eller anvendelse af oplysninger om forbrugere med henblik på markedsføring.

Efter persondatalovens § 36, stk. 1, må en virksomhed ikke videregive oplysninger om en forbruger til en anden virksomhed med henblik på markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed, hvis forbrugeren fremsætter indsigelse herimod.

Efter persondatalovens § 36, stk. 2, skal en virksomhed inden den videregiver oplysninger om en forbruger til en anden virksomhed med henblik på

markedsføring eller anvender oplysningerne på vegne af en anden virksomhed i dette øjemed, undersøge i CPR, om forbrugeren har frabedt sig henvendelser i markedsføringsøjemed. Endvidere skal virksomheden inden oplysninger om en forbruger, der ikke i CPR har frabedt sig sådanne henvendelser, videregives eller anvendes som nævnt i 1. pkt., tydeligt og på en forståelig måde oplyse om retten til at gøre indsigelse efter stk. 1. Forbrugeren skal samtidig gives adgang til på en nem måde inden for to uger at gøre sådan indsigelse.

Oplysningerne må ikke videregives, inden fristen til at gøre indsigelse er udløbet.

Efter persondatalovens § 36, stk. 3, skal en henvendelse til forbrugeren efter stk. 2 i øvrigt ske i overensstemmelse med reglerne i markedsføringslovens § 10 og regler udstedt i medfør af markedsføringslovens § 10, stk. 7. Bestemmelsen sikrer et bedre samspil mellem reglen om henvendelser til forbrugeren efter stk. 2 og markedsføringslovens regler om uanmodet direkte markedsføring.

Endvidere følger det af persondatalovens § 36, stk. 4, at virksomheden ikke kan kræve betaling for behandlingen af en indsigelse.

Bestemmelserne i persondatalovens § 36, stk. 1, stk. 2, 2. pkt., og stk. 4, er baseret på artikel 14, litra b, i databeskyttelsesdirektivet, hvorefter medlemsstaterne indrømmer den registrerede ret til efter anmodning og uden udgifter at modsætte sig en behandling af personoplysninger, der vedrører den pågældende, og som den registeransvarlige agter at foretage med henblik på markedsføring, eller at blive underrettet, inden personoplysningerne første gang videregives til tredjemand eller anvendes på tredjemands vegne med henblik på markedsføring, og udtrykkelig få tilbud om uden udgifter at gøre indsigelse mod en sådan videregivelse eller anvendelse.

Ordningen i persondatalovens § 36, stk. 2, 1. pkt., som ikke er baseret på databeskyttelsesdirektivets artikel 14 b, blev indsat for yderligere at styrke den registreredes rettigheder. Der henvises til pkt. 4.2.5.3 i de almindelige bemærkninger til lovforslag nr. L 147 af 9. december 1999 om behandling af personoplysninger.

2.4.2. Databeskyttelsesforordningen

Reglerne om de registreredes rettigheder, fremgår af databeskyttelsesforordningens kapitel III. For nærmere om oplysningspligt ved indsamling hos den registrerede, jf. forordningens artikel 13, se *betænkningen*, side 279-296, om oplysningspligt, hvis personoplysningerne ikke er indsamlet hos den registrerede, jf. forordningens artikel 14, se *betænkningen*, side 296-312 samt om indsigt retten, jf. forordningens artikel 15, se *betænkningen*, side 315-325, 373-374 samt 387-389 for en nærmere gennemgang af de registreredes rettigheder.

Disse regler vil erstatte bestemmelser herom i den gældende persondata-lov.

Databeskyttelsesforordningens artikel 21, stk. 2 og 3, regulerer den registreredes indsigelsesret over for behandling af oplysninger med henblik på direkte markedsføring.

Det følger af databeskyttelsesforordningens artikel 21, stk. 2, at den registrerede til enhver tid har ret til at gøre indsigelse mod behandling af sine personoplysninger, hvis oplysningerne behandles med henblik på direkte markedsføring, herunder at gøre indsigelse mod profilering, i det omfang den vedrører direkte markedsføring.

Efter forordningens artikel 21, stk. 3, må personoplysningerne ikke længere behandles med henblik på direkte markedsføring, hvis den registrerede gør indsigelse mod behandling til dette formål.

Ved direkte markedsføring må skulle forstås markedsføring, som er rettet direkte mod en bestemt person.

Herudover fastsætter forordningens artikel 21, stk. 4, bl.a. krav om meddelelse til den registrerede om muligheden for at gøre indsigelse efter stk. 2.

For nærmere om forordningens artikel 21, stk. 2-4, henvises til *betænkningen*, s. 366 ff.

Efter databeskyttelsesforordningens artikel 23, stk. 1, er der mulighed for ved lovgivningsmæssige foranstaltninger i EU-retten eller medlemsstaternes nationale ret at begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 12-22 og 34 samt artikel 5, for så vidt bestemmelserne heri svarer til rettighederne og forpligtelserne i artikel 12-22,

når begrænsningerne respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til en række nærmere oplistede hensyn.

Begrænsningerne kan ske af hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed, forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare, handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed, 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, beskyttelse af retsvæsenets uafhængighed og retssager, forebyggelse, efterforskning, afsløring og retsforfølgning i forbindelse med brud på etiske regler for lovregulerede erhverv, kontrol-, tilsyns- eller reguleringsfunktioner, herunder opgaver af midlertidig karakter, der er forbundet med offentlig myndighedsudøvelse i nogle af de tilfælde, der er omhandlet ovenfor, beskyttelse af den registrerede eller andres rettigheder og frihedsrettigheder og håndhævelse af civilretlige krav.

Det fremgår endvidere af databeskyttelsesforordningens artikel 23, stk. 2, at navnlig skal enhver lovgivningsmæssig foranstaltning, der er omhandlet i stk. 1, som minimum, hvor det er relevant, indeholde specifikke bestemmelser vedrørende: Formålene med behandlingen eller kategorierne af behandling, kategorierne af personoplysninger, rækkevidden af de indførte begrænsninger, garantierne for at undgå misbrug eller ulovlig adgang eller overførsel, specifikation af den dataansvarlige eller kategorierne af dataansvarlige, opbevaringsperioder og de gældende garantier under hensyntagen til behandlingens karakter, omfang og formål eller kategorier af behandling, risiciene for de registreredes rettigheder og frihedsrettigheder, og de registreredes ret til at blive underrettet om begrænsningen, medmindre dette kan skade formålet med begrænsningen.

2.4.3. Justitsministeriets overvejelser og lovforslagets udformning

2.4.3.1. Der bør efter Justitsministeriet vurdering ikke påhvile dataansvarlige en ubetinget oplysningspligt og indsichtsret over for registrerede personer, da en sådan pligt i visse situationer er uhensigtsmæssig.

Justitsministeriet vurderer således, at det er nødvendigt med mulighed for konkret at kunne begrænse oplysningspligten og indsigtsretten.

En ubetinget oplysningspligt og indsigtsret vil kunne være skadelig af hensyn til afgørende *private* interesser, herunder hensynet til vedkommende selv.

Derudover vil en ubetinget oplysningspligt og indsigtsret kunne være skadeligt af hensyn til afgørende *offentlige* interesser, herunder hensynet til statens sikkerhed eller den offentlige sikkerhed. Justitsministeriet vurderer således, at det er nødvendigt med mulighed for den dataansvarlige at undtage visse oplysninger fra oplysningspligten og indsigtsretten i forordningen efter en konkret vurdering.

Justitsministeriet vurderer derfor, at det skal være muligt konkret – i lighed med den gældende retstilstand – at undtage personoplysninger fra oplysningspligten og indsigtsretten, herunder i forbindelse med automatiske afgørelser, og at dette bør ske i det omfang databeskyttelsesforordningens artikel 23 giver mulighed herfor, se *betænkningen*, side 396-404, hvor mulighederne for begrænsning efter artikel 23 nærmere er gennemgået. Der lægges herved vægt på, at samtlige de undtagelsesmuligheder, som fremgår af disse bestemmelser, er udtryk for hensigtsmæssige begrænsninger af oplysningspligten og indsigtsretten efter forordningen.

2.4.3.2. Indsigtsretten bør efter Justitsministeriets opfattelse også tilpasses offentlighedslovens regler om egenaces.

Således foreslås det – i lighed med den gældende retstilstand – for at skabe sammenhæng mellem forordningens regler om indsigt og de gældende bestemmelser i offentlighedsloven om egenaces, jf. offentlighedslovens § 8, at forvaltningsmyndigheder i samme udstrækning som efter den nævnte bestemmelse i offentlighedsloven skal kunne gøre undtagelse fra retten til indsigt. Herved sikres det, at der er overensstemmelse mellem regler i databeskyttelsesforordningen, lovforslaget og offentlighedslovens regler om egenaces.

Justitsministeriet vurderer, at den nugældende ordning i persondatalovens 32, stk. 2, kan opretholdes på baggrund af forordningens artikel 23, se *betænkningen*, side 396-404, og artikel 86, se *betænkningen*, side 959-966.

2.4.3.3. Hvad særligt angår domstolene vurderer Justitsministeriet, at det – i lighed med den gældende retstilstand – er hensigtsmæssigt, at der ikke er ret til indsigt i oplysninger, der behandles for domstolene, hvis oplysningerne indgår i en tekst, der ikke foreligger i endelig form. Hvis oplysningerne er videregivet til en tredjemand, finder Justitsministeriet dog, at den registrerede skal have ret til indsigt i oplysningerne.

2.4.3.4. Justitsministeriet foreslår endvidere en særlig undtagelsesregel med hensyn til oplysninger, som udelukkende behandles i videnskabeligt øjemed, ligesom foreslås, at der ikke gives registrerede personer indsigt i oplysninger, som kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker. Også dette forslag er i overensstemmelse med den gældende retstilstand.

De undtagelser, som foreslås, skaber efter Justitsministeriets vurdering en rimelig balance mellem på den ene side hensynet til den registrerede og på den anden side hensynet til andre beskyttelsesværdige interesser, herunder bl.a. til, at der ikke pålægges de dataansvarlige for vidtgående byrder i forbindelse med behandlingen af oplysninger.

Der henvises i øvrigt til lovforslagets § 22 og de specielle bemærkninger hertil.

2.4.3.5. Det følger af forordningens artikel 13, stk. 3, og artikel 14, stk. 4, at hvis den dataansvarlige agter at viderebehandle personoplysningerne til et andet formål end det, hvortil de er indsamlet, giver den dataansvarlige forud for denne viderebehandling den registrerede oplysninger om dette andet formål og andre relevante yderligere oplysninger. Der er således tale om en fornyet oplysningspligt i forhold til oplysningspligten, der i øvrigt følger af artikel 13, stk. 1-2, og artikel 14, stk. 1-2.

Der henvises til *betænkningen* side 96, 293-294, og 306-307.

Oplysningspligten i forordningens artikel 13 og 14 er en central rettighed for den registrerede, der giver mulighed for at blive orienteret herom, når en dataansvarlig behandler oplysninger om én.

Set fra den dataansvarliges side kan den fornyede oplysningspligt, der nu følger af forordningens artikel 13, stk. 3 og artikel 14, stk. 4, opleves som administrativ byrdefuld. Samtidig synes det tvivlsomt, om en fornyet op-

lysningspligt i denne situation reelt vil skabe større retssikkerhed for den registrerede.

Det er på denne baggrund Justitsministeriets vurdering, at det er forsvarligt – inden for rammerne af forordningens artikel 23 – at begrænse (alene) den *fornye*de oplysningspligt efter forordningens artikel 13, stk. 3 og artikel 14, stk. 4, i *det omfang* vedkommende minister har udnyttet bemyndigelsen i lovforslagets § 5, stk. 3, og i bekendtgørelsesform bestemt, at en nærmere angiven viderebehandling af personoplysninger lovligt skal kunne finde sted i den offentlige forvaltning.

Der er derfor indsat en bestemmelse herom i lovforslagets § 23.

Herefter har den registrerede – der allerede én gang er blevet oplyst om den oprindelige behandling af personoplysninger, jf. forordningens artikel 13, stk. 1-2, og artikel 14, stk. 1-2 – mulighed for i Lovtidende nærmere at orientere sig om, at en viderebehandling af oplysninger kan finde sted. Samtidigt har den registrerede stadig ret til indsigt efter forordningens artikel 15 i den videre behandling af personoplysninger, der måtte blive foretaget på baggrund af lovforslagets § 5, stk. 3.

Justitsministeriet vurderer, at den foreslåede bestemmelse om begrænsningen af oplysningspligten efter forordningens artikel 13, stk. 3 og artikel 14, stk. 4, ligger inden for rammerne af mulighederne for at begrænse rettigheder efter forordningens artikel 23, som i stk. 1, litra e, bl.a. giver mulighed for at begrænse rettighederne af hensyn til en medlemsstats væsentlige økonomiske interesser.

Der henvises i øvrigt til lovforslagets § 23 og de specielle bemærkninger hertil.

2.4.3.6. Persondatalovens § 36, stk. 1, stk. 2, 2. pkt., og stk. 4, er baseret på databeskyttelsesdirektivets artikel 14, litra b, som afløses af databeskyttelsesforordningens artikel 21, stk. 2-4.

Bestemmelserne i databeskyttelsesforordningens artikel 21, stk. 2-4, vurderes ikke at være en ændring af gældende ret, idet indsigelsesretten i forbindelse med direkte markedsføring også følger af gældende ret. Det er dog den begrænsning i forhold til gældende ret, at der efter artikel 21, stk. 2, kun kan gøres indsigelse i forbindelse med de situationer, hvor der er tale om direkte markedsføring.

Da forordningens artikel 21, stk. 2-4, gælder direkte, foreslås bestemmelsen i persondatalovens § 36, stk. 1, stk. 2, 2. pkt., og stk. 4, ikke videreført.

Som en konsekvens foreslås § 36, stk. 3, heller ikke videreført, da den hænger sammen med bestemmelsen i § 36, stk. 2, 2. pkt.

Dog foreslås ordningen med pligtmæssig undersøgelse af CPR efter persondatalovens § 36, stk. 2, 1. pkt., videreført med tilpasninger i forhold til databeskyttelsesforordningen, således at ordningen ændres fra at gælde for *markedsføring* til at gælde for *direkte markedsføring*.

Tilpasningen vurderes ikke at indebære væsentlige ændringer i praksis i forhold til gældende ret.

Der henvises til forslagets § 13 og de specielle bemærkninger hertil.

2.5. Supplerende bestemmelser til databeskyttelsesforordningens kapitel IV

2.5.1. Gældende ret

2.5.1.1. Der er ingen bestemmelse efter gældende ret, hvorefter databeskyttelsesrådgivere, der er udpeget efter databeskyttelsesforordningens artikel 37, stk. 1, litra b og c, ikke uberettiget må videregive eller udnytte oplysninger, som de under udøvelsen af deres hverv som databeskyttelsesrådgivere er blevet bekendt med.

2.5.1.2. Der er ingen bestemmelse efter gældende ret, hvorefter det sikres, at certificeringsorganer akkrediteres af den tilsynsmyndighed, der er kompetent i henhold til artikel 55 og 56 i databeskyttelsesforordningen.

2.5.2. Databeskyttelsesforordningen

2.5.2.1. Det følger af databeskyttelsesforordningens artikel 38, stk. 5, at databeskyttelsesrådgiveren er underlagt tavshedspligt eller fortrolighed vedrørende udførelsen af sine opgaver i overensstemmelse med EU-retten eller medlemsstaternes nationale ret.

Bestemmelsen må på baggrund af ordvalget antages at overlade det til EU-retten eller medlemsstaternes nationale lovgivning, om databeskyttelsesrå-

dgiveren i det konkrete tilfælde skal være underlagt tavshedspligt eller fortrolighed. I en dansk kontekst vil det f.eks. være forvaltningslovens § 27 og straffelovens §§ 152-152 f, der medfører tavshedspligt eller fortrolighed.

Se nærmere i *betænkningen* side 583-584.

2.5.2.2. Det følger af databeskyttelsesforordningens artikel 43, stk. 1, litra a, at medlemsstaterne sikrer, at certificeringsorganer akkrediteres af den tilsynsmyndighed, der er kompetent i henhold til artikel 55 og 56 i forordningen.

Af forordningens artikel 43, stk. 1, fremgår det, at certificeringsorganer, der har et passende ekspertiseniveau for så vidt angår databeskyttelse, udsteder og forlænger certificering, efter at have underrettet tilsynsmyndigheden for at gøre det muligt for den at udøve sine beføjelser i henhold til artikel 58, stk. 2, litra h), hvis det er nødvendigt, uden at dette berører den kompetente tilsynsmyndigheds opgaver og beføjelser i henhold til artikel 57 og 58.

Det fremgår endvidere af bestemmelsen, at medlemsstaterne sikrer, at disse certificeringsorganer akkrediteres af en eller begge af følgende:

- a) den tilsynsmyndighed, der er kompetent i henhold til artikel 55 eller 56
- b) det nationale akkrediteringsorgan, som er udpeget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008⁶⁶⁹ i overensstemmelse med ENISO/IEC 17065/2012 og med de supplerende krav, der er fastsat af den tilsynsmyndighed, som er kompetent i henhold til artikel 55 eller 56.

Certificering sker således efter, at certificeringsorganet har underrettet tilsynsmyndigheden, så denne har haft mulighed for at udøve sine beføjelser i henhold til artikel 58, stk. 2, litra h, hvilket blandt andet omfatter muligheden for at give påbud om ikke at udstede en certificering.

Når overladelse af kontrollen med overholdelsen af en certificeringsmekanisme ikke berører den kompetente tilsynsmyndigheds opgaver og beføjelser, betyder dette bl.a., at tilsynsmyndigheden stadig har sine opgaver og beføjelser for så vidt angår behandlingsaktiviteter, der foregår i tilknytning til en certificeringsmekanisme, som kontrolleres af et akkrediteret organ.

Tilsynsmyndigheden kan dermed fortsat føre tilsyn med behandlingsaktiviteter, både generelt og i forhold til eventuelle specifikke områder, som måtte være omfattet af certificeringsmekanismer.

I forhold til akkreditering af et certificeringsorgan, fremgår det, at dette kan udføres af den kompetente tilsynsmyndighed eller af et nationalt akkrediteringsorgan. Når akkreditering udføres af sidstnævnte, er det vigtigt at være opmærksom på, at den kompetente tilsynsmyndighed kan stille supplerende krav.

2.5.3. Justitsministeriets overvejelser og lovforslagets udformning

2.5.3.1. Det følger af databeskyttelsesforordningens artikel 38, stk. 5, at databeskyttelsesrådgiveren skal pålægges tavshedspligt eller fortrolighed vedrørende udførelsen af sine opgaver i overensstemmelse med EU-retten eller medlemsstaternes nationale ret.

Justitsministeriet finder derfor, at er nødvendigt at indføre en sådan bestemmelse, der regulerer spørgsmålet om databeskyttelsesrådgiveres tavshedspligt.

Bestemmelsen i lovforslagets § 24 pålægger alene databeskyttelsesrådgivere, der er ansat i det private, tavshedspligt med hensyn til at videregive eller udnytte oplysninger, som de under udøvelsen af deres hverv som databeskyttelsesrådgivere er blevet bekendt med.

Denne fremgangsmåde er valgt, idet offentligt ansatte databeskyttelsesrådgivere allerede er omfattet af de almindelige regler om tavshedspligt i det offentlige efter forvaltningslovens § 27 og straffelovens § 152 og §§ 152 c-152 f.

Omvendt er private ikke som udgangspunkt omfattet af tavshedspligt, medmindre det følger af lovgivningen. Fremgangsmåden vil derfor sikre, at også databeskyttelsesrådgivere, der er ansat i det private, er underlagt tavshedspligt, når de udøver deres hverv som databeskyttelsesrådgiver.

Justitsministeriet finder, at i det omfang, der ikke i den øvrige lovgivning er regler om tavshedspligt, pålægges databeskyttelsesrådgivere, der er ansat i det private, nu tavshedspligt efter lovforslagets § 24, jf. kravet herom i forordningens artikel 38, stk. 5.

Justitsministeriet finder endvidere, at ”uberettiget” videregivelse eller udnyttelse på områder, hvor der i den øvrige lovgivning, f.eks. lov om finansiel virksomhed, er regler om tavshedspligt, skal forstås en overtrædelse af den pågældende tavshedspligt efter den øvrige lovgivning.

Der henvises i øvrigt til lovforslagets § 41, stk. 7, og bemærkningerne her-
til.

2.5.3.2. Certificering nævnes i flere af forordningens artikler om behandlingssikkerhed og har potentiale til at få stor betydning fremover. Justitsministeriet finder derfor, at der i lovforslagets § 25 bør fastsættes en regel om, at Datatilsynet er bemyndiget til at akkreditere certificeringsorganer, jf. databeskyttelsesforordningens artikel 43, stk. 1, litra a.

Justitsministeriet finder således, at det er Datatilsynet, som bemyndiges til at akkreditere certificeringsorganer bl.a. af hensyn til at skabe en klar ansvarsfordeling.

2.6. Tilladelse til behandling

2.6.1. Gældende ret

Efter persondatalovens § 50, stk. 1, skal Datatilsynets tilladelse forinden iværksættelse af en behandling, indhentes, bl.a. når behandlingen af oplysningerne sker med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret, eller behandlingen sker med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed.

Endvidere skal Datatilsynets tilladelse bl.a. indhentes, når der behandles følsomme oplysninger eller strafbare forhold for private, eller behandlingen udelukkende finder sted med henblik på at føre retsinformationssystemer.

Efter persondatalovens § 50, stk. 2, skal Datatilsynets tilladelse ved overførsel af oplysninger som nævnt i stk. 1 til tredjelande i medfør af § 27, stk. 1, og stk. 3, nr. 2-4, indhentes til overførslen, uanset at behandlingen i øvrigt er undtaget fra anmeldelse i medfør af § 49, stk. 1.

Endvidere er der i persondatalovens § 50, stk. 3 og 4, bemyndigelsesbestemmelser, hvorefter justitsministeren kan fastsætte undtagelser fra be-

stemmelserne i stk. 1, nr. 1, og stk. 2, og regler om, at der forinden iværksættelse af andre anmeldelsespligtige behandlinger end de i stk. 1 eller 2 nævnte skal indhentes tilladelse fra tilsynet.

Endelig følger det af persondatalovens § 50, stk. 5, at tilsynet i forbindelse med meddelelse af tilladelse efter stk. 1, 2 eller 4 kan fastsætte nærmere vilkår for udførelsen af behandlingerne til beskyttelse af de registreredes privatliv.

Af persondatalovens § 51, stk. 2, fremgår det, at Datatilsynets tilladelse skal indhentes forinden iværksættelse af ændringer i de i § 48, stk. 2, jf. § 43, stk. 2, nævnte oplysninger i anmeldelser af behandlinger, som er omfattet af § 50, stk. 1, 2 eller 4. Ændringer af mindre væsentlig betydning skal alene anmeldes. Anmeldelse kan ske efterfølgende, dog senest 4 uger efter iværksættelsen.

2.6.2 Databeskyttelsesforordningen

Efter databeskyttelsesforordningen er der ikke krav om, at der skal indhentes en tilladelse fra tilsynsmyndighederne inden iværksættelsen af visse typer af behandlinger, herunder i forbindelse med advarselsregistre og kreditoplysningsvirksomhed.

Det følger således af forordningens artikel 30, at den dataansvarlige og databehandleren i visse tilfælde skal føre interne fortegnelser over deres behandling af personoplysninger. Se *betænkningen* side 443-464.

Efter forordningens artikel 36, stk. 5, kan medlemsstaterne dog fastsætte nærmere regler om, at den dataansvarlige i forbindelse med visse behandlingsaktiviteter altid skal høre og opnå forudgående tilladelse fra tilsynsmyndigheden under udførelsen af en opgave i samfundets interesse. Se *betænkningen* side 537-544.

Forordningens kapitel V indeholder endelig regler om overførsler af personoplysninger til tredjelande eller internationale organisationer.

2.6.3. Justitsministeriets overvejelser og lovforslagets udformning

2.6.3.1. Bestemmelsen i lovforslagets § 26, stk. 1, foreskriver et krav om, at der skal indhentes en tilladelse fra Datatilsynet inden iværksættelsen af visse typer af behandlinger.

Der skal ske forelæggelse for Datatilsynet, før iværksættelse af advarselsregistervirksomhed, kreditoplysningsbureauvirksomhed samt ved behandling, som udelukkende finder sted med henblik på at føre retsinformationssystemer.

Databeskyttelsesforordningens artikel 30 lægger som nævnt op til en anden ordning end efter anmeldelsesordningen i gældende ret, hvorefter den dataansvarlige og databehandleren i visse tilfælde skal føre fortegnelser over deres behandling af personoplysninger.

Forordningen giver for så vidt angår behandling under udførelse af en opgave i samfundets interesse dog mulighed for, at medlemsstaterne i national ret generelt kan kræve, at den dataansvarlige hører og opnår forudgående tilladelse fra tilsynsmyndigheden, også i de tilfælde, som ellers ikke er omfattet af kravet om forudgående høring af tilsynsmyndigheden, jf. artikel 36, stk. 1.

Forordningens artikel 36, stk. 5, åbner således op for, at medlemsstaterne kan fastsætte nærmere regler om, at den dataansvarlige i forbindelse med visse behandlingsaktiviteter altid – uanset om konsekvensanalysen har vist, at behandlingen vil medføre en høj risiko i mangel af foranstaltninger eller ej – skal høre og opnå forudgående tilladelse fra tilsynsmyndigheden – altså en fravigelse af forordningens udgangspunkt om en afskaffelse af anmeldelseskravet.

Denne fravigelse af forordningens almindelige ordning, som artikel 36, stk. 5, giver rum for, er dog begrænset til behandlingsaktiviteter som led i ”udførelse af en opgave i samfundets interesse”. Som eksempler herpå nævner forordningen behandling i forbindelse med social sikring og folkesundhed. Se *betænkningen* side 541-542.

Justitsministeriet vurderer, at tilladelsesordningen for iværksættelse af advarselsregistervirksomhed, kreditoplysningsbureauvirksomhed samt ved behandling, som udelukkende finder sted med henblik på at føre retsinformationssystemer kan indeholdes inden for rammerne af artikel 36, stk. 5, og således opretholdes i dansk ret. Tilladelsesordningen vil således være i samfundets interesse, idet der lægges vægt på, at sådanne indgribende former for behandling af personoplysninger vurderes og bedømmes nærmere af Datatilsynet.

Efter Justitsministeriets vurdering er det således påkrævet at fastsætte nærmere regler om registre, der oprettes med henblik på at advare andre imod forretningsforbindelser med eller ansættelsesforhold til en registreret samt ved kreditoplysningsvirksomhed. Det er af meget væsentlig betydning for såvel enkeltpersoner som virksomheder, at registrering i advarselsregistre og behandling i et kreditoplysningsbureau sker på en saglig og lovlig måde. Ulovlige behandlinger på dette område vil kunne medføre alvorlige skadevirkninger for de involverede parter.

Efter Justitsministeriets vurdering er det endvidere efter samme hensyn påkrævet at fastsætte regler om en tilladelse ved behandling, som udelukkende finder sted med henblik på at føre retsinformationssystemer, idet der i sådanne systemer foretages en særligt indgribende behandling af personoplysninger.

Justitsministeriet vurderer, at en sådan tilladelsesordning, kombineret med muligheden for at stille vilkår, jf. stk. 4, vil være egnet til at tilvejebringe et klart og utvetydigt grundlag, på hvilket virksomheden mv. kan foretage sin behandling.

Hertil kommer, at Datatilsynet vil have mulighed for at lade en tilladelse bortfalde, hvis en virksomhed mv. tilsidesætter vilkårene eller går ud over det, som den har oplyst i anmeldelsen.

Efter Justitsministeriets vurdering bør det således overlades til Datatilsynet i hvert enkelt tilfælde at afgøre, om oprettelsen af advarselsregistre tjener anerkendelsesværdige interesser, og i bekræftende fald at give individuelle vilkår med hensyn til registrets brug.

Endelig bør det efter Justitsministeriets vurdering overlades til Datatilsynet at afgøre, hvorvidt der skal gives tilladelse til kreditoplysningsvirksomhed. For nærmere om kreditoplysningsområdet se ovenfor i afsnit 2.3.11.

2.6.3.2. Justitsministeriet vurderer ikke, at persondatalovens ordning med forudgående tilladelse fra Datatilsynet ved behandling af bl.a. følsomme oplysninger og strafbare forhold for private skal opretholdes. Dette er særligt af hensyn til, at forordningen ikke lægger op til en anmeldelsesordning, men i stedet har fokus på den risikobaserede tilgang, herunder med fortegnelseskravet.

Det bemærkes i den forbindelse, at det fremgår af forordningens præambelbetragtning nr. 89, at den generelle forpligtelse til at anmelde behandlingen af personoplysninger til tilsynsmyndighederne medføre en administrativ og finansiell byrde, men ikke i alle tilfælde bidrog til at forbedre beskyttelsen af personoplysninger. Det fremgår endvidere, at en sådan vilkårlig og generel anmeldelsespligt derfor bør afskaffes og erstattes med effektive procedurer og mekanismer, som i stedet fokuserer på de typer behandlingsaktiviteter, der sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder i medfør af deres karakter, omfang, sammenhæng og formål.

Justitsministeriet vurderer endelig, at det er mest hensigtsmæssigt, at det er forordningens regler i kapitel V om overførsel af oplysninger til tredjelande og internationale organisationer, som regulerer dette område, jf. herom *betænkningen* side 630-734.

2.6.3.3. I tilknytning til forslaget om tilladelsesordningen vurderer Justitsministeriet, at det er hensigtsmæssigt, at der i lovforslaget skal indsættes bemyndigelsesbestemmelser, ifølge hvilke justitsministeren kan fastsætte undtagelser fra kravet om tilladelse før iværksættelse af advarselsregister-virksomhed og kreditoplysningsbureauvirksomhed eller kan fastsætte regler om, at andre behandlinger skal tillades inden iværksættelsen. Justitsministeriet forudsætter i sidstnævnte tilfælde, at der er tale om behandlinger, som indebærer en særlig risiko på grund af deres art, omfang eller formål.

Når bemyndigelsen til at fastsætte regler om indhentning af tilladelse fra Datatilsynet i stk. 3 udnyttes, er det efter forordningens artikel 36, stk. 5, tillige et krav, at der skal være tale om en behandling under udførelsen af en *opgave i samfundets interesse*.

2.6.3.4. Justitsministeriet vurderer endelig, at ordningen med, at Datatilsynets tilladelse skal indhentes på ny, hvis der er tale om væsentlige ændringer, jf. lovforslagets § 26, stk. 5, skal opretholdes.

Når lovforslaget træder i kraft, vil det ikke være nødvendigt at indhente en ny tilladelse til en fortsat behandling, som Datatilsynet har givet tilladelse til efter persondatalovens § 50, stk. 1, nr. 2-3, men Datatilsynets tilladelse skal dog også fremover indhentes på ny, hvis der er tale om væsentlige ændringer.

Der henvises i øvrigt til lovforslagets § 26 og bemærkningerne hertil.

2.7. Tilsyn

Beskrivelsen nedenfor under afsnit 2.7.1. og 2.7.2. af gældende ret og af databeskyttelsesforordningen bygger navnlig på *betænkningen*, jf. herom kapitel VI og dele af kapitel VII.

2.7.1. Gældende ret

I dag varetages tilsynet med persondataloven af Datatilsynet og for domstolenes administrative forhold af Domstolsstyrelsen.

Også andre offentlige myndigheder påser overholdelsen af lovgivning, som vedrører beskyttelsen af personoplysninger, eksempelvis Finanstilsynet og Forbrugerombudsmanden.

2.7.1.1. Det fremgår af persondatalovens § 55, at Datatilsynet, der består af et råd og et sekretariat, fører tilsyn med enhver behandling, der omfattes af loven, idet tilsynet med domstolene dog varetages af Domstolsstyrelsen for så vidt angår behandling af oplysninger med hensyn til domstolenes administrative forhold, jf. nærmere herom i afsnit 2.7.1.9. nedenfor.

Datatilsynets daglige forretninger varetages af sekretariatet, der ledes af en direktør, og rådet, der 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, jf. bestemmelsens stk. 2 og 3. Rådet fastsætter sin forretningsorden og de nærmere regler om arbejdets fordeling mellem råd og sekretariat, jf. stk. 4.

Det fremgår af § 8 i forretningsordenen, jf. bekendtgørelse nr. 1178 af 15. december 2000 om forretningsordenen for Datarådet, at rådets medlemmer har tavshedspligt med hensyn til, hvad de erfarer i deres egenskab af medlem af rådet, når der er tale om oplysninger, som efter deres karakter er fortrolige. Samme tavshedspligt påhviler medarbejdere i sekretariatet, der medvirker ved rådsbehandlingen.

Datatilsynet og Domstolsstyrelsen udøver deres funktioner i fuld uafhængighed, jf. persondatalovens § 56 og § 68, stk. 1, og deres afgørelser kan ikke indbringes for anden administrativ myndighed, jf. § 61 og § 68, stk. 1, 2. pkt.

Efter persondatalovens § 58, stk. 1, og § 68, stk. 1, påser Datatilsynet og Domstolsstyrelsen af egen drift eller efter klage fra en registreret, at behandlingen af personoplysninger finder sted i overensstemmelse med loven og regler udstedt i medfør af loven.

2.7.1.2. Efter persondatalovens § 57 skal der ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger, indhentes en udtalelse fra Datatilsynet.

2.7.1.3. Efter persondatalovens § 62 kan Datatilsynet kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser. Tilsvarende gælder for Domstolsstyrelsen, jf. § 68, stk. 1.

For nærmere herom henvises til *betænkningen* side 769-773 og 788-807.

Herudover har Datatilsynets medlemmer og personale til enhver tid mod behørig legitimation uden retskendelse 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, jf. persondatalovens § 62, stk. 2. Tilsvarende gælder for Domstolsstyrelsen, jf. lovens § 68, stk. 1.

Det følger endvidere af persondatalovens § 62, stk. 3, at bestemmelsen i stk. 2 gælder tilsvarende for behandlinger, som foretages for private dataansvarlige, i det omfang behandlingen er omfattet af § 50 eller foretages i forbindelse med tv-overvågning.

I bestemmelsen er fastsat en begrænset inspektionsbeføjelse, nemlig til de typer af behandlinger, som er undergivet et krav om forudgående tilladelse samt inspektioner, der foretages i forbindelse med tv-overvågning. Dette gælder også behandlinger, som er inddraget under tilladelsesordningen i medfør af § 50, stk. 4.

Det følger endvidere af persondatalovens § 62, stk. 4, at bestemmelsen i stk. 2 også gælder, for så vidt angår den behandling, der udføres af databehandlere som nævnt i lovens § 53.

Efter persondatalovens § 62, stk. 2-4, kan der foretages inspektion i forhold til såvel behandlinger, der er omfattet af denne lov, som i forhold til behandlinger, som er omfattet af en anden medlemsstats lovgivning, jf. herved også persondatalovens § 64, stk. 1.

2.7.1.4. Efter persondatalovens § 61 kan Datatilsynets afgørelser efter loven ikke indbringes for anden administrativ myndighed.

Efter gældende ret kan Datatilsynets afgørelser til enhver tid indbringes for domstolene, jf. grundlovens § 63, hvorefter domstolene er berettigede til at påkende ethvert spørgsmål om øvrighedsmyndighedens grænser. Herudover er tilsynets virksomhed undergivet Folketingets Ombudsmands kompetence.

2.7.1.5. Efter persondatalovens § 64, stk. 2, kan Datatilsynet 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.

2.7.1.6. Efter persondatalovens § 65, sidste del, kan Datatilsynet offentliggøre sine udtalelser. Endvidere bestemmes det, at mulighed for at begrænse de registreredes rettigheder tilsvarende finder anvendelse.

For nærmere herom henvises til *betænkningen* side 807-811.

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

2.7.1.8. I persondatalovens § 63, stk. 1, er der en bestemmelse om, at Datatilsynet kan bestemme, at anmeldelser og ansøgninger om tilladelse efter persondataloven og ændringer heri kan eller skal indgives på nærmere angiven måde.

I persondatalovens § 63, stk. 2, er der en bestemmelse om, at for indgivelse af en række anmeldelser og ansøgninger om tilladelser i henhold til loven betales 2.000 kr.

Det følger endvidere af stk. 5, at såfremt en behandling både skal anmeldes efter § 48, jf. § 63, stk. 2, nr. 1 og tillades efter § 50, jf. § 63, stk. 2, nr. 2, betales kun ét gebyr.

2.7.1.9. Reglerne om tilsynet med domstolene findes i persondatalovens kapitel 17.

Som nævnt ovenfor i afsnit 2.7.1.1. fører Domstolsstyrelsen tilsyn med domstolenes behandling af personoplysninger med hensyn til administrative forhold. Domstolsstyrelsen har i den forbindelse en række af de samme beføjelser som Datatilsynet, se nærmere ovenfor i afsnit 2.7.1.3.

For anden behandling af oplysninger træffes afgørelse af vedkommende ret. Afgørelsen kan kæres til højere ret. For særlige domstole, hvis afgørelser ikke kan indbringes for højere ret, kan den nævnte afgørelse kæres til den landsret, i hvis kreds retten er beliggende. Kærefristen er 4 uger fra den dag, afgørelsen er meddelt den pågældende, jf. persondatalovens § 67, stk. 3.

2.7.2. Databeskyttelsesforordningen

Forordningens kapitel VI og kapitel VII, afdeling 1, indeholder regler om uafhængige tilsynsmyndigheder, tilsynsmyndighedernes status, opgaver og beføjelser samt regler om samarbejde mellem tilsynsmyndighederne.

Det fremgår af forordningens artikel 51, stk. 1, at en eller flere tilsynsmyndigheder skal være ansvarlige for og føre tilsyn med anvendelsen af forordningen. Den tilsynsmyndighed, som er ansvarlig for tilsynet efter databeskyttelsesforordningen, kan tillige være tilsynsmyndighed i forhold til retshåndhævelsesdirektivet, jf. direktivets § 41, stk. 3.

Forordningens artikel 52 indeholder krav om, at tilsynsmyndigheden skal udføre sine opgaver og udøve sine beføjelser i fuld uafhængighed og med de fornødne ressourcer mv. På tilsvarende måde skal medlemmer af tilsynsmyndigheden holde sig fri for udefrakommende indflydelse og fra virksomhed, som er uforenelig med hvervet, jf. bestemmelsens stk. 2 og 3.

Forordningens artikel 53 indeholder regler om de generelle betingelser for medlemmer af en tilsynsmyndighed, herunder at medlemmer skal udnævnes på baggrund af deres faglige kvalifikationer efter en gennemsigtig procedure af f.eks. parlamentet eller regeringen. Bestemmelsens stk. 3 og 4 indeholder nærmere regler om ophør af embedsperiode og om afskedigelse.

Forordningens artikel 54 indeholder en liste over de elementer forbundet med oprettelsen af en tilsynsmyndighed, hvor medlemsstaterne skal fastsætte regler. Der skal bl.a. fastsættes regler om, at embedsperioden for medlemmerne skal være på mindst fire år og regler om, hvorvidt der kan ske genudnævnelse af medlemmer. Det fremgår endvidere af bestemmelsens stk. 2, at medlemmerne skal have tavshedspligt i forhold til de oplysninger, som kommer til deres kendskab under udøvelsen af deres opgaver.

Forordningens artikel 55 indeholder regler om tilsynsmyndighedens kompetencer. Det fremgår af bestemmelsens stk. 3, at tilsynsmyndigheder ikke er kompetente til at føre tilsyn med domstolenes behandlingsaktiviteter, når de handler i deres egenskab af domstol.

Forordningens artikel 56 indeholder regler om den ledende tilsynsmyndigheds kompetence, herunder regler om, hvilken national tilsynsmyndighed, der er den ledende tilsynsmyndighed.

Forordningens artikel 57 indeholder en liste over tilsynsmyndighedens opgaver, herunder om at føre tilsyn, at rådgive på forskellige måder og behandle klager fra registrerede. Efter bestemmelsens stk. 2 skal tilsynsmyndigheden lette indgivelse af klager fra registrerede mv. gennem foranstaltninger som f.eks. en klageformular. Åbenbart grundløse eller uforholdsmæssige anmodninger kan endvidere pålægges gebyr eller afvises, jf. artikel 57, stk. 4. Tilsynsmyndigheden kan f.eks. inddrage ressourcehensyn ved vurderingen af, om en anmodning skal afvises eller pålægges et gebyr. Det vil dog kun være den del af anmodning, som er uforholdsmæssig, der kan afvises eller pålægges et gebyr.

Forordningens artikel 58 indeholder regler om tilsynsmyndighedens beføjelser, hvoraf det bl.a. følger, at tilsynsmyndigheden har beføjelse til at få indsigt i alle de personoplysninger, der behandles, og alle oplysninger, der kræves til udførelse af myndighedens opgaver.

Tilsynsmyndigheden tillægges endvidere effektive korrigerende beføjelser, f.eks. til at udstede advarsler, påbud eller forbud, jf. artikel 58, stk. 2.

Efter databeskyttelsesforordningens artikel 36, stk. 4, hører medlemsstaterne tilsynsmyndigheden som led i udarbejdelse af et forslag til lovgivningsmæssige foranstaltninger, som skal vedtages af et nationalt parlament, eller af en regulerende foranstaltning, der har hjemmel i en sådan lovgivningsmæssig foranstaltning, som vedrører behandling.

Efter forordningens artikel 58, stk. 5, fastsætter hver medlemsstat ved lov, at dens tilsynsmyndighed har beføjelser til at indbringe overtrædelser af de bestemmelser, der vedtages i henhold til forordningen, for de judicielle myndigheder og om nødvendigt at indlede eller på anden måde deltage i retssager med henblik på at håndhæve disse bestemmelser.

Efter forordningens 58, stk. 6, kan hver medlemsstat endvidere ved lov fastsætte, at dens tilsynsmyndighed har yderligere beføjelser end dem, der er omhandlet i artikel 58, stk. 1, 2 og 3. Udøvelsen af disse beføjelser må dog ikke hindre en effektiv anvendelse af kapitel VII.

Tilsynsmyndigheden skal udarbejde en årlig rapport om sin virksomhed, som skal fremsendes til det nationale parlament og regeringen samt gøres tilgængelig for offentligheden, Kommissionen og Databeskyttelsesrådet, jf. artikel 59.

Tilsynsmyndighederne skal efter forordningens artikel 60 samarbejde såvel nationalt som medlemsstaterne imellem. Bestemmelsens stk. 2-12 indeholder nærmere regler om samarbejdet mellem tilsynsmyndighederne i forskellige medlemsstater.

Tilsynsmyndighederne skal efter forordningens artikel 61 udveksle relevante oplysninger og yde hinanden gensidig bistand med henblik på at gennemføre og anvende forordningen på en ensartet måde. Bestemmelsens stk. 2-9 indeholder nærmere regler om gensidig bistand mellem tilsynsmyndighederne i forskellige medlemsstater, herunder regler om, at anmodninger skal besvares uden unødigt forsinkelse og senest en måned efter modtagelsen, jf. stk. 2, og at en anmodning kun kan afvises, hvis den modtagende tilsynsmyndighed ikke har kompetence til at udføre den, eller en imødekommelse ville være i strid med forordningen eller med EU-ret eller national ret, som den modtagende tilsynsmyndigheder er underlagt.

Tilsynsmyndighederne skal efter forordningens artikel 62 gennemføre fælles aktiviteter, hvis det er hensigtsmæssigt.

Der henvises til *betænkningen* side 739-832.

2.7.3. Justitsministeriets overvejelser og lovforslagets udformning

Forordningens kapitel VI og kapitel VII, afdeling 1, indeholder regler om uafhængige tilsynsmyndigheder, tilsynsmyndighedernes status, opgaver og beføjelser samt regler om samarbejde mellem tilsynsmyndighederne. Reglerne er sammenfaldende med reglerne om tilsynsmyndigheden i lov om retshåndhævende myndigheders behandling af personoplysningers kapitel VIII.

2.7.3.1. I forhold til Datatilsynets organisation foreslår Justitsministeriet i vidt omfang en videreførelse af den gældende ordning.

Dette indebærer, at Datatilsynet har tilsynskompetence på alle områder inden for dansk jurisdiktion omfattet af forordningen og lovforslagets 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. Øvrige tilsyn, såsom Finanstilsynet og Forbrugerombudsmanden, der ikke har status som uafhængige tilsynsmyndigheder, vil have karakter af supplerende tilsyn i forhold til Datatilsynets generelle tilsyn.

Det er et krav efter forordningens artikel 54, stk. 1, litra e, at medlemsstaterne fastsætter regler om, hvorvidt der kan ske genudnævnelse af medlemmer af tilsynsmyndigheden, og i givet fald hvor mange gange, at der kan ske genudnævnelse.

Justitsministeriet vurderer, at hensynet til at sikre en vis kontinuitet for Datarådet, og til at sikre, at rådets medlemmer opnår tilstrækkelig erfaring med behandling af rådets sager, taler for, at der skal være mulighed for genudnævnelse.

På den anden side vil en ubegrænset adgang til genudnævnelse – såfremt en sådan ordning ville være i overensstemmelse med forordningen – kunne skabe tvivl om medlemmets uafhængighed, idet det ville kunne anføres, at medlemmet agerer på en måde i rådet, som er egnet til at sikre, at der sker genudnævnelse af den pågældende.

Justitsministeriet vurderer, at en ordning, hvor der er mulighed for at blive genudnævnt to gange, udgør en fornuftig balance mellem disse to hensyn.

Justitsministeriet vurderer desuden, at karakteren af de oplysninger, som vil kunne tilgå rådet, kan begrunde, at der fremover stilles krav om, at rå-

dets formand, medlemmer og stedfortrædende medlemmer kan sikkerhedsgodkendes, og at sikkerhedsgodkendelsen kan opretholdes i hele embedsperioden. En sådan ordning er i overensstemmelse med forordningens artikel 53, stk. 4, hvorefter et medlem bl.a. kan afskediges, hvis den pågældende ikke længere opfylder betingelserne for at varetage sit hverv.

Det bemærkes, at medarbejdere ved Datatilsynet også fortsat vil skulle sikkerhedsgodkendes i overensstemmelse med Justitsministeriets cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret).

I forhold til forordningens krav om, at den enkelte tilsynsmyndigheds medlem eller medlemmer og personale såvel under som efter deres embedsperiode skal have tavshedspligt for så vidt angår alle fortrolige oplysninger, der er kommet til deres kendskab under udførelsen af deres opgaver eller udøvelsen af deres beføjelser, jf. artikel 54, stk. 2, er det Justitsministeriets vurdering, at dette krav er opfyldt gennem Datarådets forretningsorden, jf. afsnit 2.7.1.1 ovenfor, forvaltningslovens § 27 og straffelovens § 152.

For så vidt angår spørgsmålet om tilsynsmyndighedernes uafhængighed, som er reguleret i forordningens artikel 52, er der tale om en videreførelse af gældende ret, herunder udtryk for en kodificering af EU-Domstolens retspraksis om fortolkningen af de krav til tilsynsmyndighedens uafhængighed, som følger af databeskyttelsesdirektivet.

Den gældende ordning i Danmark efter persondatalovens §§ 55 og 56 og §§ 67 og 68 med Datatilsynets og Domstolsstyrelsens tilsyn anses for at leve op til det gældende uafhængighedskrav.

Justitsministeriet forholdt sig således til tilsynsmyndighedernes uafhængighed i et svar af 17. december 2012 på spørgsmål nr. 284 (Alm. del) af 19. november 2012 fra Folketingets Retsudvalg. Det fremgår af besvarelsen, at det af persondatalovens § 56 følger, at Datatilsynet udøver sine funktioner i fuld uafhængighed. Dette indebærer bl.a., at hverken Justitsministeriet eller andre ministerier kan give instruktioner eller føre tilsyn med Datatilsynet.

Det fremgår endvidere af besvarelsen, at det af forarbejderne til persondataloven (Folketingstidende 1999-2000, tillæg A, side 4101) fremgår, at der ved udpegning af medlemmer af rådet skal tilstræbes uvildighed og sagkundskab, og at rådets medlemmer således skal udpeges på en måde, der sikrer Datatilsynet den fornødne uafhængighed. Hvad angår de ansatte i Datatilsynets sekretariat er disse ikke undergivet et tjenstligt tilsyn fra Justitsministeriets side.

Den foreslåede § 27 omfatter således tillige de aspekter af uafhængighedskravet, som er anført i forordningens artikel 52, stk. 2-6. I forhold til spørgsmålet om tilsynsmyndighedens budget, som efter forordningens artikel 52, stk. 6, skal være særskilt, kan det bemærkes, at bevillingen til Datatilsynet og Domstolsstyrelsen fremgår særskilt af den årlige finanslov under Justitsministeriet.

Der henvises i øvrigt til lovforslagets § 27 og bemærkningerne hertil.

2.7.3.2. Justitsministeriet vurderer, at der skal indsættes en bestemmelse i lovforslagets § 28 om, at ved udarbejdelse af lovforslag, bekendtgørelser, cirkulærer eller lignende generelle retsfor skrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger, skal der indhentes en udtalelse fra Datatilsynet.

Justitsministeriet vurderer, at det er hensigtsmæssigt, at denne bestemmelse indsættes, idet regulering alene efter forordningens artikel 36, stk. 4, se *betænkningen* side 538-544, kan give tvivl om, hvorvidt cirkulærer vil være omfattet af høringspligten. Bestemmelsen er således indsat for at sikre, at cirkulærer fremadrettet også vil være omfattet af høringspligten.

Der henvises i øvrigt til lovforslagets § 28 og bemærkningerne hertil.

2.7.3.3. Justitsministeriet foreslår, at bestemmelsen i persondatalovens § 62, stk. 1, om 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 videreføres i lovforslagets § 29, stk. 1.

Med hensyn til spørgsmålet om inspektionskompetence foreslår Justitsministeriet, at der fastsættes en bestemmelse om, at tilsynets medlemmer og personale mod behørig legitimation til enhver tid uden retskendelse har adgang til alle lokaler, hvorfra en behandling af personoplysninger foretages, jf. lovforslagets § 29, stk. 2.

Bestemmelsen er fastsat på grundlag af forordningens artikel 58, stk. 1, litra f, hvoraf det følger, at hver tilsynsmyndighed har undersøgelsesbeføjelse til 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.

Bestemmelsen i stk. 2, som tager sigte på alle lokaler, hvorfra behandling af personoplysninger foretages, svarer delvist til persondatalovens § 62, stk. 2-4. Bestemmelsen giver dog på baggrund af forordningens artikel 58, stk. 1, litra f, en udvidet adgang til lokaler hos private, da forordningen ikke giver mulighed for at fastsætte bestemmelser om begrænsning af inspektionsbeføjelser svarende til persondatalovens § 62, stk. 3.

Justitsministeriet vurderer, at den foreslåede bestemmelse i § 29, stk. 2, er inden for rammerne i forordningens artikel 58, stk. 1, litra f.

Justitsministeriet vurderer, at det er hensigtsmæssigt, at der opretholdes en bestemmelse om, 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, databeskyttelsesforordningen eller den pågældende medlemsstats databeskyttelseslovgivning.

Justitsministeriet vurderer, at det med ordningen i lovforslagets § 29 sikres, at Datatilsynet – ligesom i dag – vil kunne føre et effektivt tilsyn med overholdelsen af lovgivningen.

Der henvises i øvrigt til lovforslagets § 29 og bemærkningerne hertil.

2.7.3.4. Afgørelser truffet af Datatilsynet bør efter Justitsministeriets opfattelse ikke kunne indbringes for anden administrativ myndighed, jf. lovforslagets § 30, stk. 1, som svarer til persondatalovens § 61. Reglen gælder bl.a. afgørelser truffet efter forordningens artikel 58.

Bestemmelsen er ikke til hinder for, at afgørelserne indbringes for Folketingets Ombudsmand.

Samtidig bør Datatilsynets spørgsmål om overtrædelser af lovforslaget efter Justitsministeriets opfattelse kunne indbringes for retten i den borgerlige retsplejes former.

Denne retstilstand følger allerede i vidt omfang af gældende ret, idet Datatilsynets afgørelser til enhver tid kan indbringes for domstolene, jf. grundlovens § 63, hvorefter domstolene er berettigede til at påkende ethvert spørgsmål om øvrighedsmyndighedens grænser.

Bestemmelsen i stk. 2 er indsat på baggrund af forordningens artikel 58, stk. 5, hvorefter det følger, at hver medlemsstat ved lov fastsætter, 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.

Der henvises i øvrigt til lovforslagets § 30 og bemærkningerne hertil.

2.7.3.5. Justitsministeriet foreslår en bestemmelse i lovforslagets § 31 om, at hvis der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet efter artikel 45 i databeskyttelsesforordningen, kan Datatilsynet i særlige tilfælde forbyde, begrænse eller suspendere overførsel af særlige kategorier af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, til et tredjeland eller en international organisation.

Bestemmelsen er fastsat på grundlag af forordningens artikel 49, stk. 5, som giver mulighed for, at grænserne for overførsel kan fastsættes i medlemsstaternes nationale ret af hensyn til vigtige samfundsinteresser.

Justitsministeriet vurderer, at Datatilsynet i særlige tilfælde bør have mulighed for at kunne udnytte den mulighed til at forbyde, begrænse eller suspendere overførsel af følsomme oplysninger til et tredjeland eller en international organisation, som forordningen giver mulighed for.

Der henvises i øvrigt til lovforslagets § 31 og bemærkningerne hertil.

For nærmere herom henvises til *betænkningen* side 732-734.

2.7.3.6. Databeskyttelsesforordningens kapitel VII indeholder regler om samarbejde mellem tilsynsmyndighederne i EU. Det må antages, at forordningens artikel 61 og 62 om gensidig bistand og fælles aktiviteter ikke udtømmende gør op med, hvilke muligheder, der er for at samarbejde, hvorfor der også vil være mulighed for at samarbejde på andre måder. Se nærmere *betænkningen* side 821-831.

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 forordningen på en ensartet måde og træffer foranstaltninger med henblik på et effektivt samarbejde med hinanden.

Justitsministeriet vurderer derfor, at den foreslåede bestemmelse er inden for rammerne i forordningen.

Der henvises i øvrigt til lovforslagets § 32 og bemærkningerne hertil.

2.7.3.7. Justitsministeriet vurderer, at ordningen i den foreslåede § 33 med, at Datatilsynet kan offentliggøre sine udtalelser, er hensigtsmæssigt, hvorfor denne foreslås opretholdt. Justitsministeriet vurderer endvidere, at det – særligt af hensyn til afgørende hensyn til private interesser – er nødvendigt, at tilsynets ret og pligt til at undlade at offentliggøre oplysninger efter lovforslagets § 22 opretholdes.

Justitsministeriet vurderer endvidere, at den foreslåede bestemmelse i § 33, er inden for rammerne i forordningen, herunder forordningens artikel 58, stk. 6, se nærmere i *betænkningen* side 806.

Der henvises i øvrigt til lovforslagets § 33 og bemærkningerne hertil.

2.7.3.8. Justitsministeriet vurderer, at det er nødvendigt, at ordningen med, at Datatilsynet og Domstolsstyrelsen samarbejder, i det omfang det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle relevante oplysninger, som svarer til persondatalovens § 66, opretholdes.

Justitsministeriet vurderer således, at det bør være fastsat ved lov, at Datatilsynet og Domstolsstyrelsen kan samarbejde i det omfang, det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle relevante oplysninger. Dette særligt fordi Datatilsynet er i besiddelse af en betydelig sagkundskab vedrørende databeskyttelsesretlige spørgsmål, som det bør være muligt for Domstolsstyrelsen at trække på.

Der henvises i øvrigt til lovforslagets § 34 og bemærkningerne hertil.

2.7.3.9. Justitsministeriet vurderer, at der på grundlag af forordningens artikel 58, stk. 6 – hvorefter hver medlemsstat ved lov kan fastsætte, at dens tilsynsmyndighed har yderligere beføjelser end dem, der er omhand-

let i stk. 1, 2 og 3 – bør fastsættes en bemyndigelse hertil for Justitsministeren.

Efter lovforslagets § 35 kan Justitsministeren således fastsætte nærmere regler om, at Datatilsynet og Domstolsstyrelsen har yderligere beføjelser end dem, der er omhandlet i databeskyttelsesforordningens artikel 58, stk. 1, 2 og 3.

Justitsministeriet vurderer, at denne mulighed bør udnyttes, idet det ikke kan afvises, at der vil opstå behov for at fastsætte yderligere beføjelser til Datatilsynet og Domstolsstyrelsen.

Der henvises i øvrigt til lovforslagets § 35 og bemærkningerne hertil.

2.7.3.10. Justitsministeriet foreslår, at den nugældende ordning med, at Datatilsynet kan bestemme, at ansøgninger om tilladelse efter loven og ændringer heri kan eller skal indgives på nærmere angiven måde, opretholdes. Justitsministeriet vurderer, at ordningen herom er hensigtsmæssig af hensyn til, at Datatilsynet kan fungere effektivt.

Justitsministeriet foreslår endvidere bestemmelser i forslagets § 36, *stk. 2 og 3*, hvorefter Justitsministeren kan fastsætte nærmere regler om betaling af gebyr for indgivelse af ansøgninger om tilladelser i henhold til denne lov, samt regler om betaling af gebyr efter databeskyttelsesforordningens artikel 57, stk. 4.

Det følger af forordningens artikel 57, stk. 4, at 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.

Den foreslåede ordning i stk. 2 med betaling af et gebyr findes også i persondatalovens § 63, stk. 2, hvorefter der for indgivelse af en række anmeldelser om ansøgninger om tilladelse i henhold til loven betales 2.000 kr.

Justitsministeriet vurderer, at det er hensigtsmæssigt, at muligheden for at opkræve et gebyr for visse anmodninger, opretholdes.

Derudover vurderer Justitsministeriet, at det er hensigtsmæssigt, at der fastsættes en selvstændig bemyndigelse til justitsministeren til at fastsætte regler om betaling af gebyr for efter forordningens artikel 57, stk. 4.

Som anført i *betænkningen* side 788, antages det i dansk ret, at der i almindelighed kræves lovhjemmel for, at en myndighed kan kræve gebyrer for at udføre deres opgaver. Justitsministeriet vurderer, at dette krav opfyldes ved den foreslåede bestemmelse i § 36, stk. 2-3.

Justitsministeriet vurderer endvidere, at det vil være hensigtsmæssigt, at selve muligheden for at fastsætte regler om gebyrer mv. bemyndiges justitsministeren, særligt af hensyn til, at dette vil resultere i en hurtigere og smidigere mulighed for bl.a. at regulere gebyrets størrelse.

Der henvises i øvrigt til lovforslagets § 36 og bemærkningerne hertil.

2.7.3.11. Tilsynsmyndigheden har efter forordningen ikke kompetence til at føre tilsyn med domstolenes behandlingsaktiviteter, når de handler i deres egenskab af domstol.

Justitsministeriet foreslår på den baggrund, at ordningen efter persondatalovens § 67 videreføres, hvorefter Domstolsstyrelsen alene har kompetence til at føre tilsyn med domstolenes behandling af personoplysninger med hensyn til administrative forhold.

Justitsministeriet vurderer, at lovforslagets § 29 om, at tilsynsmyndigheden kan kræve enhver oplysning, der er af betydning for deres virksomhed samt ordningen med, at tilsynsmyndighedens medlemmer og personale mod behørig legitimation har adgang til alle lokaler uden retskendelse, skal finde anvendelse, når Domstolsstyrelsen udøver tilsyn. For nærmere se afsnit 2.7.3.3. Dette er nødvendigt for, at Domstolsstyrelsen kan føre det fornødne tilsyn.

Endvidere vurderer Justitsministeriet, at bestemmelsen om Datatilsynets og Domstolsstyrelsens samarbejde også bør finde anvendelse for Domstolsstyrelsen. For nærmere se afsnit 2.7.3.8..

Domstolsstyrelsens tilsyn bør således efter Justitsministeriets opfattelse i det væsentlige svare til, hvad der foreslås i relation til Datatilsynet.

2.8. Retsmidler, ansvar og sanktioner

2.8.1. Gældende ret

2.8.1.1. Det følger af persondatalovens § 40, at den registrerede kan klage til vedkommende tilsynsmyndighed over behandling af oplysninger vedrørende den pågældende. Denne bestemmelse har alene informativ karakter. 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.

Det følger af persondatalovens § 58, stk. 1, der også er baseret på direktivets artikel 28, stk. 4, 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.

Der henvises til *betænkningen* side 862-866, om gældende ret vedrørende retten til at klage til tilsynsmyndigheden.

2.8.1.2. Retsplejeloven fastsætter reglerne for, hvordan og hvornår den registrerede har adgang til domstolsprøvelse af, om dennes rettigheder er blevet krænkede som følge af en overtrædelse af reglerne i persondataloven og databeskyttelsesdirektivet.

For at kunne anlægge en sag ved domstolene, herunder mod tilsynsmyndigheden eller mod en dataansvarlig 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.

Der henvises til *betænkningen* side 869-874 og 878-880, om gældende ret vedrørende den registreredes adgang til domstolsprøvelse over for en tilsynsmyndighed og over for en dataansvarlig eller en databehandler.

2.8.1.3. Efter § 69 skal den dataansvarlige erstatte skade, der er forvoldt ved behandling i strid med bestemmelserne i loven, medmindre det godtgøres, at skaden ikke kunne have været afværget ved den agtpågivenhed og omhu, der må kræves i forbindelse med behandling af oplysninger.

Der er således tale om et præsumptionsansvar (culpa med omvendt bevisbyrde) for den dataansvarlige. Erstatningsansvaret reguleres i øvrigt af de almindelige erstatningsretlige principper.

Det fremgår af forarbejderne til persondataloven (Folketingstidende 1999-2000, tillæg A, side 4043 f.), at valget af præsumptionsansvar som ansvarsgrundlag var påkrævet for at sikre en korrekt implementering af databeskyttelsesdirektivet.

Der henvises til *betænkningen* side 898-909, om erstatning for overtrædelse af persondataloven.

2.8.1.4. 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 strafpålægte.

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.

Persondatalovens § 70, stk. 2, indeholder regler om straf i forbindelse med behandling, som udføres for offentlige myndigheder. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller hæfte den, der overtræder § 41, stk. 3 (om behandlingssikkerhed), eller § 53 (om forudgående anmeldelse for databehandlere) eller tilsidesætter vilkår som nævnt i § 7, stk. 7 (om behandling af følsomme oplysninger), § 9, stk. 3 (om førelse af retsinformationssystemer), § 10, stk. 3 (om videregivelse af følsomme oplysninger og oplysninger om rent private forhold til tredje mand i statistisk eller videnskabeligt øjemed), § 13, stk. 1 (om registrering af udgående telefonopkald), § 27, stk. 4 (overførsel af oplysninger til tredje lande), eller en betingelse eller et vilkår for en tilladelse i henhold til regler udstedt i medfør af loven.

Det fremgår videre af persondatalovens § 70, stk. 5, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Det fremgår af straffelovens § 27, stk. 2, at statslige myndigheder og kommuner alene kan straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private.

Der henvises til *betænkningen* side 918-920 og 938-943, om gældende ret vedrørende den registreredes adgang til domstolsprøvelse over for en tilsynsmyndighed og over for en dataansvarlig eller en databehandler.

2.8.2. Databeskyttelsesforordningen

2.8.2.1. 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.

Der henvises til *betænkningen* side 866-868, om retten til at klage til tilsynsmyndigheden efter databeskyttelsesforordningen.

2.8.2.2. 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.

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.

Der henvises til *betænkningen* side 875-878 og 880-883, om forordningens regler om den registreredes adgang til domstolsprøvelse over for en tilsynsmyndighed og over for en dataansvarlig eller en databehandler.

2.8.2.3. 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.

Der henvises til *betænkningen* side 888-891, om forordningens regler om den registreredes adgang til at lade sig repræsentere.

2.8.2.4. 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.

Der henvises til *betænkningen* side 910-918, for den nærmere analyse af rækkevidden af forordningens artikel 82 om erstatning.

2.8.2.5. Sanktionen for overtrædelser af bestemmelserne i databeskyttelsesforordningen er i medfør af artikel 83 administrative bøder, som tilsynsmyndigheden sanktionerer.

Databeskyttelsesforordningens artikel 83, stk. 1-6, indeholder således en række generelle betingelser for pålæggelse af administrative bøder. Med denne bestemmelse er tilsynsmyndigheden forpligtet til at sanktionere de

administrative overtrædelser, der er anført i artikel 83 og pålægge bøder under hensynstagen til de konkrete omstændigheder i hver sag.

Indførelsen af administrative bøder giver i dansk ret betænkeligheder i forhold til grundloven. I dansk retspleje er det dog et grundlæggende princip, at bøder, der har karakter af strafferetlig sanktion, kun kan idømmes ved domstolene og i strafferetsplejens former, der sikrer den sigtede en effektiv beskyttelse. Datatilsynet bør dermed ikke få 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.

Dog kan der gives mulighed for, at Datatilsynet kan udstede bødeforelæg i egnede sager.

Det fremgår derfor af forordningens præambelbetragtning nr. 151, at reglerne om administrative bøder i forordningen i Danmark kan anvendes ved, at bøder idømmes 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.

Muligheden for at vælge strafferetlige sanktioner frem for administrative bøder følger af databeskyttelsesforordningen artikel 83, stk. 9, 1. pkt. Det fremgår af denne bestemmelse, at hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, kan bestemmelsen 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 tilsynsmyndigheden.

På den baggrund bør sanktioner for overtrædelser af forordningens bestemmelser efter dansk ret fastsættes som en strafferetlig sanktion, jf. artikel 83, stk. 9, 1. pkt., jf. artikel 83, stk. 1-6.

For så vidt angår strafferetlige sanktioner for overtrædelser af forordningen, indeholder artikel 83, stk. 1-3, en række generelle betingelser for idømmelse af strafferetlige sanktioner, herunder hvilke principper, der skal iagttages, og hvilke momenter, der har betydning for idømmelse af bøder og -størrelse.

Forordningens artikel 83, stk. 4–6, fastlægger, hvilke af forordningens bestemmelser, der kan idømmes bøde for overtrædelse af og den maksimale bødestørrelse for de pågældende overtrædelser.

Det følger således af databeskyttelsesforordningens artikel 83, *stk. 4*, at overtrædelse af følgende bestemmelser straffes med bøder på op til 10.000.000 euro, 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 endvidere af databeskyttelsesforordningens artikel 83, *stk. 5*, at overtrædelse af følgende bestemmelser straffes i overensstemmelse med stk. 2 med bøder på op til 20.000.000 euro, 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 forpligtelser 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.

Endelig følger det 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 bøder på op til 20.000.000 euro, 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.

Ud over de af forordningens bestemmelser, der nævnes i artikel 83, stk. 4-6, kan medlemsstaterne fastsætte regler om andre sanktioner, der skal anvendes i tilfælde af overtrædelser af forordningen, jf. artikel 84, stk. 1.

Medlemsstaterne er efter denne bestemmelse 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.

Databeskyttelsesforordningen indeholder endvidere en forpligtelse i artikel 84, stk. 1, for medlemsstaterne til at fastsætte regler om andre sanktioner, navnlig end pålæggelse af administrative bøder, jf. artikel 83, 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 overtrædelserne og have afskrækkende virkning. Det betyder, at medlemsstaterne skal fastsætte nationale regler om andre sanktioner end administrative bøder.

For så vidt angår straffniveauet for overtrædelser af flere bestemmelser i forordningen, fremgår det af 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 forordningen, må bødens samlede størrelse ikke overstige beløbet for den alvorligste overtrædelse.

2.8.3. Justitsministeriets overvejelser og lovforslagets udformning

2.8.3.1. Forordningens artikel 77 indeholder et krav om, at enhver registreret har ret til at indgive klage til en tilsynsmyndighed.

Bestemmelsen svarer til den gældende bestemmelse i persondatalovens § 40, som foreslås videreført.

Der henvises i øvrigt til lovforslagets § 39, stk. 1, og bemærkningerne her til.

2.8.3.2. Forordningens artikel 78 indeholder regler om, at den registrerede skal have adgang til at indbringe en tilsynsmyndigheds afgørelser for domstolene. Der skal endvidere være adgang for den registrerede til at indbringe tilsynet for domstolene, hvis tilsynet har undladt at opfylde sine opgaver efter forordningen i forhold til den registrerede, dvs. ikke har behandlet

en klage eller givet underretning om forløbet eller resultatet af en klage inden for tre måneder.

For så vidt angår spørgsmålet om adgangen til at indbringe en tilsynsmyndigheds afgørelser for domstolene, følger det af grundlovens § 63, at domstolene er berettiget til at påkende ethvert spørgsmål om øvrighedsmyndighedens grænser. Denne mulighed for domstolsprøvelse vil bl.a. kunne udnyttes, såfremt Datatilsynet eller Domstolsstyrelsen har behandlet en klage fra en registreret person. I givet fald vil den registrerede, som tilsynsmyndighedens afgørelse måtte gå imod, kunne indbringe denne for domstolene.

For så vidt angår adgangen til at indbringe en tilsynsmyndighed for domstolene for ikke at have opfyldt sine opgaver, følger adgangen til at indbringe tilsynsmyndigheden for domstolene af retsplejelovens almindelige regler, hvorefter offentlige myndigheder kan sagsøges af personer med retlig interesse i spørgsmålet.

For så vidt angår spørgsmålet om, hvor en sag mod Datatilsynet eller Domstolsstyrelsen skal anlægges, fremgår det af retsplejelovens § 240, stk. 1, at staten har hjemting i den retskreds, hvor den myndighed, som stævnes på statens vegne, har kontor.

Det foreslås på den baggrund, at der fastsættes en regel om, at den registrerede kan indbringe tilsynsmyndighedens afgørelser, undladelser af at behandle en klage fra en registreret eller en manglende underretning om forløbet eller resultatet af en klage inden for tre måneder, for retten i den borgerlige retsplejes former, dvs. efter retsplejelovens regler om civile søgsmål.

Den foreslåede bestemmelse er således en videreførelse af gældende ret.

Der henvises i øvrigt til lovforslagets § 39, stk. 2, og bemærkningerne her til.

2.8.3.3. Efter forordningens artikel 79 skal den registrerede have adgang til effektive retsmidler over for en dataansvarlig eller en databehandler.

Adgangen til at indbringe tilsynsmyndigheden for domstolene, hvilket anses for at opfylde kravet om adgang til effektive retsmidler, følger af

retsplejelovens almindelige regler, jf. det ovenfor i afsnit 2.8.1.2. anførte om adgangen til at indbringe tilsynsmyndighederne for domstolene.

Det foreslås på den baggrund, at der fastsættes regler om, at den registrerede kan indbringe spørgsmål om den dataansvarliges og databehandlers overholdelse af loven for domstolene i overensstemmelse i den borgerlige retsplejes former, dvs. efter retsplejelovens regler om civile søgsmål.

Der henvises i øvrigt til lovforslagets § 39, stk. 2 og 3, og bemærkningerne hertil.

2.8.3.4. Efter forordningens artikel 80 skal den registrerede have adgang til at lade sig repræsentere i forhold til klager til tilsynsmyndigheden og indbringelse af henholdsvis tilsynsmyndighederne samt dataansvarlige og databehandlere for domstolene. Denne ret er efter forordningen begrænset til et organ, en organisation eller en sammenslutning, der er etableret i overensstemmelse med medlemsstaternes 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.

Retten til at lade sig repræsentere er efter gældende ret ikke begrænset på en måde, som svarer til forordningens artikel 80, jf. *betænkningen* side 891.

Således gælder der i dansk forvaltningsret på ulovbestemt grundlag et grundlæggende princip om, at den, der er part i en sag ved den offentlige forvaltning, på ethvert tidspunkt kan lade sig repræsentere eller bistå af andre. For så vidt angår afgørelsessager er dette princip kodificeret i forvaltningslovens § 8, stk. 1. Den, som optræder som repræsentant, skal kunne godtgøre, at vedkommende er berettiget hertil.

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. 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 tilbagekalde.

Justitsministeriet finder ikke grundlag for at indsnævre de registreredes adgang til at lade sig repræsentere i sager omfattet af lovforslagets område i forhold til dansk rets almindelige regler herom.

Det foreslås på den baggrund, at der fastsættes regler om, at den registrerede tillige skal have adgang til at udøve sine rettigheder gennem en repræsentant.

Der henvises i øvrigt til lovforslagets § 39 og bemærkningerne hertil. Der henvises også til gennemgangen i *betænkningen* side 883-891, om forordningens artikel 80 om repræsentation af registrerede.

For så vidt angår mulighederne efter artikel 8 a, stk. 2, skal Justitsministeriet bemærke, at reglerne om gruppesøgsmål i vidt omfang bygger på Retsplejerådets betænkning nr. 1468/2005 om reform af den civile retspleje IV (gruppesøgsmål mv.).

Retsplejerådet pegede i sin betænkning på en række betænkeligheder ved at tillade gruppesøgsmål efter frameldingsmodellen – de såkaldte ”opt-out”-spørgsmål – og anbefalede på baggrund heraf bl.a., at kun offentlige myndigheder skulle kunne udpeges som grupperepræsentant i sådanne gruppesøgsmål. Rådet pegede i den forbindelse bl.a. på, at offentlige myndigheder er underlagt et almindeligt saglighedskrav, når de skal vurdere, om der er grundlag for at anlægge et gruppesøgsmål. Justitsministeriet tilsluttede sig Retsplejerådets synspunkter.

Justitsministeriet udarbejdede i 2014 en redegørelse om erfaringerne med reglerne om gruppesøgsmål på baggrund af en høring af relevante myndigheder og organisationer mv. Det blev i redegørelsen konkluderet, at der ikke var behov for ændringer af reglerne om gruppesøgsmål i retsplejeloventen eller øvrige regler af betydning for sådanne spørgsmål.

Henset til Retsplejerådets overvejelser og anbefalinger og i lyset af redegørelsen fra 2014, finder Justitsministeriet ikke anledning til at foreslå ændringer af de gældende regler om gruppesøgsmål, således at private organisationer mv. kan udpeges som grupperepræsentant i gruppesøgsmål efter frameldingsmodellen.

2.8.3.5. Forordningens artikel 82 fastsætter regler om retten til erstatning og om dataansvarliges og databehandlers erstatningsansvar. Af stk. 1 fremgår, 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.

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.

Efter den gældende bestemmelse i persondatalovens § 69 skal den dataansvarlige erstatte skade, der er forvoldt ved behandling i strid med bestemmelserne i loven, medmindre det godtgøres, at skaden ikke kunne have været afværget ved den agtpågivenhed og omhu, der må kræves i forbindelse med behandling af oplysninger.

Efter de gældende regler gælder der således et skærpet ansvarsgrundlag i form af præsumptionsansvar (culpa med omvendt bevisbyrde). I modsætning til et almindeligt culpaansvar, hvor den skadelidte har bevisbyrden for, at skadevolderen har handlet culpøst, indebærer præsumptionsansvaret, at skadevolderen har bevisbyrden for, at vedkommende ikke har handlet ansvarspådragende. Efter den gældende bestemmelse i persondatalovens § 69 skal den dataansvarlige således bevise, at hverken den pågældende selv eller nogen, for hvis fejl den dataansvarlige i givet fald er ansvarlig for, har handlet culpøst. Herudover finder de almindelige erstatningsretlige principper anvendelse.

Det fremgår af forarbejderne til persondataloven, jf. lovforslag nr. L 147 af 9. december 1999 (Folketingstidende 1999-2000, tillæg A, side 4043 f.), at valget af præsumptionsansvar som ansvarsgrundlag var påkrævet for at sikre en korrekt implementering af databeskyttelsesdirektivet.

Der henvises i øvrigt til lovforslagets § 40 og bemærkningerne hertil.

2.8.3.6. I forordningens artikel 83, stk. 4-6, følger en detaljeret EU-regulering af, hvilke handlinger og undladelser, der skal være strafbare. Herudover angives den maksimale bødestørrelse for overtrædelser af forordningens forskellige bestemmelser.

Justitsministeriet finder, at det i lovforslaget bør fastsættes, hvilke bestemmelser i forordningen og loven, som er strafbelagt ved overtrædelser. På den måde kan der skabes klarhed over, hvilke bestemmelser i forordningen, der er strafferetligt sanktioneret.

På denne baggrund foreslår Justitsministeriet, at overtrædelser af følgende bestemmelser i forordningen – som oplistet i artikel 83, stk. 4 og 5 – skal kunne sanktioneres strafferetligt i lovforslaget:

- 1) den dataansvarliges og databehandlerens forpligtelser i henhold til artikel 8, 11, 25-39 og 42 og 43
- 2) certificeringsorganets forpligtelser i henhold til artikel 42 og 43
- 3) kontrolorganets forpligtelser i henhold til artikel 41, stk. 4.
- 4) de grundlæggende principper for behandling, herunder betingelserne for samtykke, i artikel 5, 6, 7 og 9
- 5) de registreredes rettigheder i henhold til artikel 12-22
- 6) overførsel af personoplysninger til en modtager i et tredjeland eller en international organisation i henhold til artikel 44-49
- 7) denne lovs §§ 9-13 og §§ 20-11
- 8) 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.

Herudover finder Justitsministeriet, at det skal være muligt at straffe dataansvarlige eller databehandlere, der undlader at efterkomme påbud fra tilsynet efter databeskyttelsesforordningens artikel 58, stk. 2, som oplistet i forordningens artikel 83, stk. 6.

Ud over de af forordningens bestemmelser, der nævnes i artikel 83, stk. 4-6, skal medlemsstaterne fastsætte regler om andre sanktioner, der skal anvendes i tilfælde af overtrædelser af forordningen, jf. artikel 84, stk. 1.

For så vidt angår betingelserne for lovlig behandling i medfør af forordningen, skal Justitsministeriet bemærke, at artikel 10 om behandling af personoplysninger vedrørende straffedomme og lovovertrædelser ikke ses at være omfattet af forordningens strafbestemmelse i artikel 83.

Justitsministeriet finder, at overtrædelser af artikel 10 om behandling af oplysninger vedrørende straffedomme og lovovertrædelse bør kunne straffes i samme omfang som overtrædelser af de øvrige behandlingsregler i forordningen, herunder behandling af følsomme og ikke-følsomme oplysninger.

Justitsministeriet finder det derfor nødvendigt at tilføje overtrædelser af behandlingsgrundlaget i artikel 10 til dette forslag.

2.8.3.7. For så vidt angår de strafferetlige sanktioner finder Justitsministeriet, at det i overensstemmelse med det grundlæggende princip i dansk retspleje om strafferetlige sanktioner og som følge af muligheden i forordningens artikel 83, stk. 9, 1. pkt., bør fastsættes i lovforslaget, at overtrædelser af de pågældende bestemmelser i forordningen og loven skal kunne sanktioneres med bøde.

Endvidere finder Justitsministeriet, at det i overensstemmelse med artikel 84, stk. 1, bør fastsættes i lovforslaget, at de pågældende overtrædelser endvidere skal kunne straffes med fængsel indtil 6 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Justitsministeriet foreslår derfor, at overtrædelser af de i lovforslagets anførte bestemmelser i forordningen straffes med bøde eller fængsel indtil 6 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Med denne fremgangsmåde finder Justitsministeriet, at Datatilsynet som forudsat i forordningen har mulighed for at tage skridt til idømmelse af bøder ved, at tilsynet på grundlag af de konstaterede overtrædelser af forordningens bestemmelser overvejer, hvorvidt der kan idømmes bøde og i så fald dennes størrelse. Såfremt Datatilsynet i en konkret sag vurderer, at der kan idømmes en bøde for de pågældende overtrædelser, indgiver tilsynet politianmeldelse sammen med en redegørelse for tilsynsmyndighedens vurdering, herunder niveauet for bøden.

Det vil herefter være politiet og anklagemyndigheden, der vurderer, hvorvidt man vil rejse tiltale i sagen.

Justitsministeriet finder endvidere, at det bør fremgå udtrykkeligt af loven, at databeskyttelsesforordningens artikel 83, stk. 2, skal følges ved idømmelse af straf i medfør af lovforslaget. Artikel 83, stk. 2, litra a-k, indeholder en række hensyn, der i hver enkelt sag skal tages behørigt hensyn til, ved idømmelse af bøde. I den forbindelse henledes særligt opmærksomheden på den ikke-udtømmende karakter af artikel 83, stk. 2, jf. bestemmelsens litra e, som åbent henviser til ”andre skærpende eller formildende faktorer ved sagens omstændigheder”.

Justitsministeriet bemærker endvidere, at straffelovens kapitel 10 om straffens fastsættelse i øvrigt finder anvendelse, medmindre bestemmelser heri strider mod databeskyttelsesforordningens artikel 83, stk. 2.

Strafudmålingen vil bero på domstolenes konkrete vurdering i det enkelte tilfælde af samtlige omstændigheder i sagen, og det angivne strafniveau vil derfor kunne fraviges i op- eller nedadgående retning, hvis der i den konkrete sag foreligger skærpende eller formildende omstændigheder, jf. hermed de almindelige regler om straffens fastsættelse i straffelovens kapitel 10.

Dog finder Justitsministeriet, at det er en afgørende forudsætning i forordningens artikel 83, stk. 9, hvorefter der kan idømmes strafferetlige sanktioner *frem for* administrative bøder, at virkningen i den danske fremgangsmåde svarer til virkningen af bøder, som administrativt pålægges af tilsynsmyndigheder i andre EU-lande.

Justitsministeriet finder derfor, at det i den danske fremgangsmåde skal sikres, at niveauet af bøder svarer til de andre EU-landes.

Justitsministeriet skal hertil bemærke, at Datatilsynet skal høres i sager, inden der træffes afgørelse om tiltaleespørgsmålet. Denne høring skal omfatte en redegørelse for tilsynets vurdering, herunder niveauet for bøder – også i forhold til niveauet i andre EU-lande.

Det indebærer, at politiet skal høre Datatilsynet inden der træffes afgørelse om tiltaleespørgsmålet i sager, der anmeldes eller kommer til politiets kendskab uden om Datatilsynet og ligeledes i sager, der bygger på Datatilsynets anmeldelse til politiet. Høringssvaret fra Datatilsynet skal tillægges vægt, når det skal vurderes, om der skal rejses tiltale.

Herudover skal Justitsministeriet bemærke, at det fremgår af forordningens artikel 83, stk. 9, at bøder under alle omstændigheder skal være effektive og stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Justitsministeriet finder på denne baggrund – og som følge af det betydelige maksimale bødebeløb i forordningen – at der med lovforslaget lægges op til en væsentlig forøgelse af bødeniveauet for overtrædelser af forordningens bestemmelser i forhold til, hvad overtrædelser af persondataloven i dag takseres til.

I forhold til det nuværende bødeniveau efter persondataloven finder Justitsministeriet således, at bødeniveauet med lovforslaget bør forhøjes væsentligt.

Justitsministeriet skal hertil bemærke, at overtrædelser af persondataloven i dag straffes med bøder på mellem 2.000 og 25.000 kr., afhængigt af karakteren af de pågældende overtrædelser.

For så vidt angår strafniveauet for overtrædelser af flere bestemmelser i forordningen, fremgår det af forordningens 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 forordningen, må bødens samlede størrelse ikke overstige beløbet for den alvorligste overtrædelse.

Der vil være grundlag for, at straffen stiger til fængsel i tilfælde, hvor der f.eks. sker en forsætlig offentliggørelse af særligt beskyttelsesværdige oplysninger, såsom følsomme oplysninger, i et meget betydeligt omfang.

Der henvises i øvrigt til lovforslagets § 41.

2.8.3.8. Med lovforslagets § 42 foreslår Justitsministeriet, at Datatilsynet bemyndiges til i sager om overtrædelse af lovforslaget, databeskyttelsesforordningen eller regler udstedt i medfør af loven at udstede administrative bødeforelæg, hvis sagerne er ukomplicerede og uden bevismæssige tvivlsspørgsmål.

Forslaget har til hensigt at indføre mulighed for en hurtig og enkel afslutning af en strafsanktioneret databeskyttelsessag.

Forslaget giver således Datatilsynet kompetence til at afslutte en sag ved udstedelse af et administrativt bødeforelæg. Forslaget retter sig kun mod sager, hvor den dataansvarlige eller databehandleren tilstår det strafbare forhold. Yderligere finder Justitsministeriet, at kompetencen er begrænset til de tilfælde, hvor sagen er egnet hertil, dvs. ukomplicerede sager og uden bevismæssige tvivlsspørgsmål.

For så vidt angår sager, der kan anses for egnede til at blive afsluttet ved udstedelse af et administrativt bødeforelæg, kan nævnes sager om utilsigtet offentliggørelse af oplysninger på internettet. Sådanne sager er karakteriseret ved, at man ved en fejl er kommet til at offentliggøre oplysninger på internettet. Det bemærkes, at der her forventes et større antal ensartede sager.

I tilfælde hvor den, der har begået overtrædelsen ikke erklærer sig rede til at betale bøden inden en nærmere angivet frist, vil domstolene afgøre bødespørgsmålet. I sådanne tilfælde vil Datatilsynet skulle indgive politianmeldelse sammen med en redegørelse for tilsynsmyndighedens vurdering, herunder niveauet for bøden.

Der henvises i øvrigt til lovforslagets § 42 og de specielle bemærkninger hertil.

2.8.3.9. Endelig finder Justitsministeriet, at den gældende § 71 i persondataloven – om frakendelse af retten til at drive eller beskæftige sig med kreditoplysningsbureauvirksomhed, advarselsregistre og edb-servicebureauer mv. – i videst mulige omfang skal videreføres, tilpasset i den mere begrænsede tilladelsesordning, der nu lægges op til efter lovforslagets § 26.

Der henvises i øvrigt til lovforslagets § 43 og de specielle bemærkninger hertil.

3. Økonomiske og administrative konsekvenser for det offentlige

4. Økonomiske og administrative konsekvenser for erhvervslivet mv.

5. Administrative konsekvenser for borgerne

Lovforslaget indebærer, at de registrerede generelt får flere rettigheder, og der sker derfor en udvidelse af de registreredes muligheder for at klage til tilsynsmyndighederne over den behandling af personoplysninger, som foretages af de kompetente myndigheder.

Lovforslaget indebærer endvidere, at de registrerede har mulighed for at udøve deres rettigheder gennem tilsynsmyndighederne.

Lovforslaget indebærer herudover, at de registrerede skal underrettes, hvis der sker brud på persondatasikkerheden, som sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder.

6. Miljømæssige konsekvenser

Lovforslaget har ikke miljømæssige konsekvenser.

7. Forholdet til EU-retten

Lovforslaget supplerer den generelle forordning nr. 2016/679 om beskyttelse af personoplysninger, som skal gælde i både den private og offentlige sektor (databeskyttelsesforordningen), der anvendes fra den 25. maj 2018.

8. Hørte myndigheder og organisationer mv.

Et udkast til lovforslaget har i perioden fra den 7. juli 2017 til den 22. august 2017 været sendt i høring hos følgende myndigheder og organisationer mv.:

Advokatrådet, Akademikernes Centralorganisation, Amnesty International, Andelsboligforeningernes Fællesrepræsentation, Arbejderbevægelsens Erhvervsråd, Arkitektforeningen, ATP, BL – Danmarks Almene Boliger, Boligselskabernes Landsforening, Copenhagen Business School (CBS), Danmarks Idræts Forbund, Danmarks Jurist- og Økonomforbund, Danmarks Lejerforeninger, Danmarks Radio, Danmarks Rederiforening, Danmarks Tekniske Universitet, Dansk Arbejdsgiverforening, Dansk Byggeri, Dansk Ejendomsmæglerforening, Dansk Erhverv, Dansk Industri, Dansk Inkassobranche, Dansk IT, Dansk Journalistforbund, Dansk Ældreråd, Danske Advokater, Danske Forlag, Danske Handicaporganisationer, Danske Insolvensadvokater, Danske Medier, Danske Regioner, Danske Seniorer, Danske Udlejere, Datatilsynet, Lægeforeningen, Den Danske Dommerforening, Det Centrale Handicapråd, Det Danske Voldgiftsinstitut, Det Kriminalpræventive Råd, Direktoratet for Kriminalforsorgen, Dommerfuldmægtigforeningen, Domstolenes Tjenestemandsförening, Domstolsstyrelsen, Ejendomsforeningen Danmark, Erhvervslejerens Landsorganisation, Experian, FAB – Foreningen af byplanlæggere, Fagligt Fælles Forbund – 3F, Finans og Leasing, Finansrådet, FOA – Fag og Arbejde, Forbrugerombudsmanden, Forbrugerrådet, Foreningen af miljø-, plan- og naturmedarbejdere i det offentlige (EnviNa), Foreningen af Offentlige Anklagere, Foreningen af Statsadvokater, Foreningen af Statsforvaltningsjurister, Foreningen Industriel Retsbeskyttelse, Forsikring og Pension, Forsikringsmæglerforeningen, FSR, Funktionærernes og Tjenestemændenes Fællesråd FTF, Færøernes Landsstyre, Grundejeren.dk, Grønlands Selvstyre, Handelshøjskolen – Århus Universitet, HK Kommunal, HK - Landsklubben Danmarks Domstole, HK Landsklubben for Politiet, Højesteret, Håndværksrådet, Indsamlingsorganisationernes Brancheorganisation, Ingeniørforeningen i Danmark, Institut for Menneskerettigheder, IT-Branchen, Justitia, KL, Kreativitet og Kommunikation, Kræftens bekæmpelse, Københavns Universitet, Landsforeningen af Forsvarsadvoka-

ter, Landsforeningen KRIM, Landsorganisationen i Danmark (LO), Lejernes Landsorganisation, Liberale Erhvervs Råd, Lægemiddelindustriforeningen (LIF), Natur- og Miljøklagenævnet, Parcelhusejernes Landsforening, Politidirektørforeningen, Politiforbundet, Postnord AB, PROSA, Procesbevillingsnævnet, Realkreditforeningen, Realkreditrådet, Retspolitisk Forening, Rigsadvokaten, Rigsombudsmanden i Grønland, Rigsombudsmanden på Færøerne, Rigspolitiet, Rådet for Digital Sikkerhed, Rådet for Etniske Minoriteter, samtlige byretter, samtlige kommuner, samtlige ministerier, samtlige regioner, Sammenslutningen af lokale Radio og Tv-stationer DFS, SikkerhedsBranchen, Syddansk Universitet, Sø- og Handelsretten, Tinglysningsretten, TV2, Udvalget til Beskyttelse af Videnskabeligt Arbejde, Vestre Landsret, Ældre Forum, Ældre Sagen, Østre Landsret, Aalborg Universitet, Aarhus Retshjælp og Aarhus Universitet.

9. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang)
Økonomiske konsekvenser for stat, kommuner og regioner		
Administrative konsekvenser for stat, kommuner og regioner		
Økonomiske konsekvenser for erhvervslivet		
Administrative konsekvenser for erhvervslivet		

Administrative konsekvenser for borgerne	Øgede muligheder for at klage til tilsynsmyndighederne, adgang til at udøve retighederne gennem tilsynsmyndighederne og underretning ved brud på persondatasikkerheden	Lovforslaget har visse negative administrative konsekvenser for borgerne.
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget supplerer den generelle forordning nr. 2016/679 om beskyttelse af personoplysninger, som skal gælde i både den private og offentlige sektor (databeskyttelsesforordningen), der anvendes fra den 25. maj 2018.	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Det fastsættes med bestemmelsens *stk. 1*, at loven supplerer og gennemfører Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, jf. bilag til denne lov.

Med bestemmelsens *stk. 2* fastsættes det, at lovforslaget og databeskyttelsesforordningen finder anvendelse på *al* behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling og på anden ikke automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, *medmindre* lovforslaget udtrykkeligt undtager nærmere bestemte former for anvendelse af personoplysninger.

Bestemmelsen indebærer, at al automatisk behandling er omfattet af loven og databeskyttelsesforordningen, medmindre det er undtaget i loven. Begrebet ”automatisk databehandling” er sammenfaldende med ”edb” eller

”elektronisk behandling”, som anvendes i databeskyttelsesdirektivets artikel 3, stk. 1.

Justitsministeriet finder, at det med denne fremgangsmåde slås fast, at forordningen vil gælde på alle livsområder med undtagelse af aktiviteter vedrørende statens sikkerhed efter artikel 3, stk. 2, litra a, og de øvrige områder, der er nævnt i forordningens artikel 3, stk. 2, litra b-d.

Der henvises i øvrigt til lovforslagets almindelige bemærkninger, afsnit 2.1., og til *betænkningen* side 31-34 og 37

I bestemmelsens *stk. 3* fastsættes det udtrykkeligt, at regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, går forud for reglerne i denne lov.

Der kan i den forbindelse henvises til *betænkningen* side 161-162, hvoraf det bl.a. fremgår, at efter databeskyttelsesforordningen vil vurderingen af lovligheden af en behandling således skulle tage sig udgangspunkt i forordningen, der som nævnt giver mulighed for nationalt at fastsætte yderligere betingelser for lovlig behandling, f.eks. at fastsætte en retlig forpligtelse.

I bestemmelsens *stk. 4* fastsættes, at der ved ”databeskyttelsesforordningen” skal forstås: Europa-Parlamentets og Rådets forordning nr. 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).

Til § 2

I denne bestemmelse fastsættes lovforslagets og databeskyttelsesforordningens anvendelsesområde, og dette udvides til at omfatte behandling af oplysninger, som ikke uden videre er omfattet af forordningens anvendelsesområde.

Justitsministeriet finder, at der på en række af de områder, der i dag er omfattet af persondatalovens § 1, stk. 2-8, også i fremtiden bør være en databeskyttelsesretlig regulering.

I bestemmelsens *stk. 1* foreslås derfor, at lovens § 8, § 10 og § 11, stk. 1, samt databeskyttelsesforordningens artikel 5, stk. 1-3, artikel 6, artikel 9 og artikel 10 også gælder for manuel videregivelse af personoplysninger til en anden forvaltningsmyndighed. Datatilsynet fører i overensstemmelse med lovens kapitel 10 tilsyn med videregivelse som nævnt i bestemmelsens stk. 1, 1. pkt.

Bestemmelsen indebærer, at den gældende ordning efter persondatalovens § 1, stk. 3, videreføres.

Hermed fastsættes det, at det vil være de anførte bestemmelser i loven og databeskyttelsesforordningen, der regulerer adgangen til manuelt at videregive personoplysninger til en anden forvaltningsmyndighed. Det bemærkes, at det ved opregningen af, hvilke bestemmelser der finder anvendelse på den nævnte manuelle videregivelse, undgås, at der opstår tvivl om, hvilke bestemmelser i loven og forordningen der gælder for denne videregivelse.

Det vil naturligvis alene være de dele af de opregnede bestemmelser i loven og databeskyttelsesforordningen, som omhandler videregivelse mellem forskellige forvaltningsmyndigheder, der vil gælde for den nævnte manuelle videregivelse. Hertil kommer, at opregningen af, hvilke bestemmelser i loven og forordningen der skal gælde for manuel videregivelse af personoplysninger til en anden forvaltningsmyndighed, vil indebære, at lovens og forordningens øvrige bestemmelser ikke vil gælde for den nævnte manuelle videregivelse.

Det er både adgangen til manuelt at videregive fortrolige og ikke-fortrolige oplysninger, der – i overensstemmelse med ordningen i persondatalovens § 1, stk. 3 – foreslås omfattet af reguleringen i de nævnte bestemmelser i loven og forordningen. Oplysninger af fortrolig karakter vil bl.a. kunne være oplysninger om race, religion, strafbare forhold, helbredsforhold og væsentlige sociale problemer, der alle er oplysninger om enkeltpersoners rent private forhold, eller oplysninger af almindelig fortrolig karakter som bl.a. oplysninger om enkeltpersoners indtægts- og formueforhold. Almindelige adresseoplysninger er et eksempel på en oplysning, som ikke er fortrolig.

Af den foreslåede bestemmelse fremgår, at det alene er adgangen til (manuelt) at videregive personoplysninger mellem *forvaltningsmyndigheder*, der foreslås omfattet af loven og databeskyttelsesforordningen.

Med den foreslåede bestemmelses 2. punktum følger det, at Datatilsynet skal føre tilsyn med manuel videregivning af personoplysninger til en anden forvaltningsmyndighed.

For så vidt angår bestemmelsens *stk. 2* fastsættes det, at loven og databeskyttelsesforordningen gælder for behandling af oplysninger om virksomheder mv., hvis denne behandling udføres for kreditoplysningsbureauer. Tilsvarende gælder for så vidt angår behandlinger, som er omfattet af lovforslagets § 26, stk. 1, nr. 1, om tilladelse vedrørende advarselsregistre.

Med bestemmelsen videreføres den gældende ordning efter persondatalovens § 1, stk. 4.

Omfattet af udtrykket ”virksomheder m.v.” er alle former for erhvervsvirksomheder, erhvervsdrivende, institutioner, foreninger og lignende, uanset om der er tale om en juridisk person eller ej. Bestemmelsen omfatter således også oplysninger om enkeltmandsejede virksomheder, uanset at sådanne oplysninger, der må anses for at være personoplysninger, tillige falder ind under lovens almindelige anvendelsesområde, således som dette er fastsat i § 1.

I bestemmelsens *stk. 3* fastsættes, at lovforslagets kapitel 4 om videregivning til kreditoplysningsbureauer af oplysninger om gæld til det offentlige også gælder for behandling af oplysninger om virksomheder mv., jf. § 1, stk. 1.

Reglerne i kapitel 4 gælder, uanset at der er tale om videregivning af automatisk behandlede oplysninger, eller om videregivning af oplysninger, der hidrører fra et manuelt register, jf. § 1, stk. 2. Baggrunden for bestemmelsen er, at spørgsmålet om en dataansvarlig forvaltningsmyndigheds adgang til at videregive de nævnte oplysninger ikke bør afhænge af, om oplysningerne er behandlet automatisk eller hidrører fra et manuelt register.

I bestemmelsens *stk. 4* fastsættes, at loven og databeskyttelsesforordningen gælder for enhver form for behandling af personoplysninger i forbindelse med tv-overvågning.

Bestemmelsen indebærer, at private og offentlige myndigheders behandling af personoplysninger i forbindelse med tv-overvågning omfattes af loven og databeskyttelsesforordningen, uanset om der finder elektronisk databehandling sted, og uanset om personoplysninger, som tilvejebringes gennem tv-overvågning, skal indgå i et register eller gøres til genstand for anden ikke-elektronisk behandling.

I bestemmelsens *stk. 5* fastsættes det, at loven og forordningen finder anvendelse for personoplysninger om afdøde personer i 10 år efter vedkommendes død

Samtidig lægger Justitsministeriet i *stk. 6* op til, at Justitsministeriet efter forhandling med vedkommende minister bemyndiges til at kunne fastsætte regler om, at loven og databeskyttelsesforordningen skal finde anvendelse på afdøde personer i en længere eller kortere periode end angivet i *stk. 5*.

Bestemmelsen sikrer, at den nævnte behandling, hvis der findes at være et behov herfor, kan reguleres efter de regler i loven og forordningen, som efter deres indhold vedrører behandling af oplysninger om afdøde personer.

Når loven og forordningen som udgangspunkt finder anvendelse på personoplysninger om afdøde personer i 10 år efter vedkommendes død, indebærer dette bl.a., at allerede behandlede oplysninger efter personens død fortsat vil være omfattet af loven og forordningen, og at indsamling og efterfølgende behandling af oplysninger om afdøde personer også skal opfylde lovens betingelse.

Dog skal det bemærkes, at en række af lovforslagets regler i sagens natur ikke kan finde anvendelse i forbindelse med behandling af oplysninger om afdøde personer. Det gælder f.eks. regler, der forudsætter den registreredes samtykke og reglerne om oplysningspligt over for den registrerede i databeskyttelsesforordningens artikel 13 og 14.

Efter bestemmelsens *stk. 7* bemyndiges Justitsministeren efter forhandling med vedkommende minister til at kunne fastsætte regler om, at lovens regler helt eller delvist skal finde anvendelse på behandling af oplysninger om virksomheder mv., som udføres for private.

Herved sikres det, at den nævnte behandling, hvis der findes at være et behov herfor, kan reguleres efter de regler i loven, som efter deres indhold vedrører behandling, som udføres for private.

Efter bestemmelsens *stk. 8* kan vedkommende minister fastsætte regler om, at lovens regler skal finde anvendelse på behandling af oplysninger om virksomheder m.v., som udføres for den offentlige forvaltning.

Herved sikres det, at den nævnte behandling, hvis der findes at være et behov herfor, kan reguleres efter de regler i loven, som efter deres indhold vedrører behandling, som udføres for den offentlige forvaltning.

Til § 3

Af bestemmelsens *stk. 1* følger, at loven og databeskyttelsesforordningens kapitel II-VII ikke finder anvendelse, hvis det vil være i strid med artikel 10 i Den Europæiske Menneskerettighedskonvention og artikel 11 i Den Europæiske Unions charter om grundlæggende rettigheder.

Der er med bestemmelsen lagt op til, at lovforslaget og databeskyttelsesforordningen i vidst mulig omfang viderefører de gældende regler i persondatalovens § 2, stk. 2-10.

Der henvises i øvrigt til lovforslagets almindelige bemærkninger.

Det drejer sig bl.a. om bestemmelsens *stk. 2*, hvorefter loven og databeskyttelsesforordningen ikke finder anvendelse på den behandling af personoplysninger, som udføres for eller af politiets og forsvarrets efterretnings-tjenester. Bestemmelsen indebærer, at den gældende ordning efter persondatalovens § 2, stk. 10 videreføres.

I forhold til *stk. 3* om Folketinget bemærkes, at i modsætning til persondataloven må forordningen antages at finde anvendelse for Folketinget og institutioner under Folketinget.

Justitsministeriet finder, at loven og databeskyttelsesforordningen skal finde anvendelse på Folketinget, når der ikke sker parlamentarisk arbejde og betjening.

Justitsministeriet foreslår, at loven og databeskyttelsesforordningen ikke finder anvendelse på den behandling af personoplysninger, der foretages

som led i Folketingets parlamentariske arbejde, herunder den betjening af Folketingets medlemmer, som Folketingets Administration foretager.

Der henvises i øvrigt til *betænkningen* side 32 og 948-958.

For så vidt angår bestemmelsens *stk. 4-8* lægges der op til, at den gældende ordning vedrørende mediernes behandlinger af oplysninger videreføres i videst muligt omfang med lovforslaget. Bestemmelserne svarer således til de gældende undtagelsesbestemmelser i persondatalovens § 2, *stk. 5-9*. Det bemærkes i den forbindelse, at forordningens kapitel III vil finde anvendelse.

For så vidt angår de uredigerede fuldtekstdatabaser, jf. forslagens *stk. 5* og *6*, og de manuelle arkiver, jf. *stk. 7*, fastsættes, at de almindelige regler om behandlingssikkerhed i forordningens artikel 32 og reglerne om databehandling i artikel 28 finder anvendelse.

Af bestemmelsens *stk. 8, 1. pkt.* følger, at for behandling af oplysninger, som i øvrigt udelukkende finder sted i journalistisk øjemed, gælder alene bestemmelserne i databeskyttelsesforordningens artikel 28 (databehandling) og 32 (behandlingssikkerhed).

Bestemmelsen tager sigte på den automatiske behandling af personoplysninger, som udelukkende foretages som led i journalistisk virksomhed i forbindelse med udarbejdelse af artikler m.v. under anvendelse af almindelige tekstbehandlingssystemer.

Det bemærkes, at databaser m.v. alene vil kunne undtages fra lovens område i det omfang, det følger af undtagelsesbestemmelserne lovens *stk. 4-8*.

Af bestemmelsens *stk. 8, 2. pkt.* følger, 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 bl.a. til »skønlitterær virksomhed«, f.eks. udarbejdelse af nøgleromaner, se hertil *betænkningen* side 952-953.

De nævnte regler gælder alene for behandling af oplysninger, som udelukkende finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed. Hvis behandlingen ikke kan anses for udelukkende at ske til de nævnte formål, finder loven og forordningens regler fuldt ud anvendelse.

Det er ikke 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. Der påhviler således den pågældende en vis forpligtelse til at sandsynliggøre, at vedkommendes aktiviteter falder ind under undtagelsesreglen. Datatilsynet - og i sidste ende domstolene - vil kunne gribe ind over for misbrug af reglen.

Der henvises i øvrigt *betænkningen* side 948-958.

Efter bestemmelsens *stk. 9* foreslås det, at Justitsministeriet efter forhandling med vedkommende minister kan fastsætte regler om, at personoplysninger, der behandles i nærmere bestemte IT-systemer, og som føres af eller for den offentlige forvaltning, alene må *opbevares* her i landet.

Bestemmelsen skal afløse den såkaldte »krigsregel« efter persondatalovens § 41, stk. 4, hvorefter der for oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Det er hensigten med reglen, at IT-systemer – før de tages i brug - af justitsministeriet og vedkommende minister kan sættes på listen, der optages som bilag til bekendtgørelsen i medfør af stk. 9.

Det er også hensigten, at IT-systemer alene sættes på denne liste, hvis det er vurderet, at det er af hensyn til *statens sikkerhed*, at det pågældende system skal føres her i landet.

I en sådan situation vil *opbevaringen* af de pågældende personoplysninger falde uden for EU-retten og dermed databeskyttelsesforordningen, jf. artikel 2, stk. 2, litra a.

Det er ikke hensigten, at bestemmelsen skal anvendes for at imødekomme hensyn, der vedrører *IT-sikkerheden*, idet dette hensyn i tilstrækkelig grad må forventes tilgodeset i bestemmelserne i forordningen, herunder artikel 32 om behandlingssikkerhed – uafhængigt af om det pågældende IT-system føres her i landet eller i et andet EU-land.

Efter bestemmelsens *stk. 10* bemyndiges Forsvarsministeriet til at kunne fastsætte regler om, at loven og databeskyttelsesforordningen helt eller

delvist ikke finder anvendelse på Forsvarets behandling af personoplysninger i forbindelse med Forsvarets internationale operative virke.

Både før, under og efter internationale operationer vil Forsvaret have behov for at behandle personoplysninger vedrørende operationerne. Det gælder særligt i forbindelse med aktiviteter af efterretningsmæssig karakter, hvor formålet bl.a. er at identificere og vurdere konkrete angrebsmål eller afdække trusler mod danske styrker fra aktører i nærområdet. Endvidere foretages der f.eks. behandlinger af personoplysninger i forbindelse med Forsvarets sikkerhedsundersøgelser af lokale samarbejdspartnere, adgangskontrol til baser, identifikation af sårede og døde samt ved optegnelser over frihedsberøvede. Disse aktiviteter sker både under de enkelte operationer og ved øvelser og uddannelse forud for udsendelse af personel til en international operation. I de regler, der fastsættes i medfør af bestemmelsen, vil disse typer af behandling af personoplysninger kunne undtages fra databeskyttelsesforordningen og lovens bestemmelser.

Det vil være uden betydning, om behandlingen af personoplysninger sker i Danmark eller i udlandet. Det afgørende vil være, at der er tale om behandling, som sker i forbindelse med Forsvarets internationale operative virke, hvilket f.eks. også vil kunne omfatte aktiviteter af efterretningsmæssig karakter og øvrige forberedende eller understøttende aktiviteter, der foretages af Forsvaret i Danmark eller i tredjelande før, under eller efter en konkret operation. Udover disse aktiviteter i Danmark og udlandet er også Forsvarets deltagelse i øvelser, operativt partnersamarbejde og lignende i udlandet omfattet af bestemmelsen.

Bestemmelsen omfatter derimod ikke mere generelle behandlinger af personoplysninger, f.eks. ved administrativ sagsbehandling af almindelige personalesager eller erstatningssager, der ikke har en direkte tilknytning til internationale operationer. Bestemmelsen omfatter derudover ikke Forsvarets deltagelse i arbejdet i internationale organisationer som f.eks. NATO, hvis dette arbejde ikke har operativ karakter.

Den militære anklagemyndigheds behandling af personoplysninger i forbindelse med bl.a. efterforskning og retsforfølgning af strafbare handlinger vil fortsat være omfattet af lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger.

Med denne bestemmelse fastsættes regler om lovens geografiske område.

Justitsministeriet finder, at lovforslaget bør gælde for dataansvarlige og databehandlere, der er *etableret* i Danmark. Bestemmelsen indebærer, at den ordning, der kendes i dag fra persondatalovens § 4, stk. 1, videreføres med lovforslaget.

Bestemmelsen lægger sig helt op ad det geografiske anvendelsesområde for forordningen således, at det geografiske område for forordningen og loven er sammenfaldende.

For så vidt angår den øvrige danske særregulering, der omfattes af forordningens materielle anvendelsesområde, må det territoriale anvendelsesområde afgøres på baggrund af den pågældende lovgivning.

De foreslåede bestemmelser berører ikke spørgsmålet om strafferetlig jurisdiktionskompetence. Dette spørgsmål vil således fortsat skulle afgøres efter reglerne i straffelovens kapitel 2.

Af bestemmelsens *stk. 2* følger, at danske diplomatiske repræsentationer er omfattet af loven og regler udstedt i medfør af loven.

Af bestemmelsens *stk. 3, litra a*, følger, at loven og regler udstedt i medfør af loven gælder for behandling af personoplysninger om registrerede, der befinder sig i Danmark, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i EU, hvis behandlingsaktiviteten vedrører udbud af varer eller tjenester til sådanne registrerede, der befinder sig i Danmark, uanset om betaling fra den registrerede er påkrævet.

Bestemmelsens *stk. 3, litra b*, fastsætter ligeledes, at loven og regler udstedt i medfør af loven gælder for behandling af personoplysninger om registrerede, der befinder sig i Danmark, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i EU, hvis behandlingsaktiviteten vedrører for behandlingsaktiviteter vedrørende overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Danmark.

Til § 5

Bestemmelsens *stk. 1* svarer til databeskyttelsesforordningens artikel 5, stk. 1, litra b. Gengivelsen i bestemmelsen er en beskrivelse af det grundlæggende princip i artikel 5, stk. 1, litra b, hvorefter følger, at personop-

lysninger skal indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål.

For så vidt angår bestemmelsens *stk. 2* er der tale om en gengivelse af muligheden for genanvendelse af personoplysninger efter forordningens artikel 6, stk. 4, 2. led, litra a-e.

Der er *ikke* med gengivelsen i bestemmelsen tiltænkt en ændring af princippet i forordningens artikel 6, stk. 4, 2. led, litra a-e.

Der henvises i øvrigt til afsnit 2.3.1.3 i lovforslagets almindelige bemærkninger og *betænkningen* side 96.

Anvendelsen af ”ikke-uforenelighedstesten” i bestemmelsens *stk. 2* forudsætter i udgangspunktet en konkretiseret vurdering af, hvorvidt en behandling ikke er uforenelig med det oprindelige formål.

I forhold til bestemmelsens *stk. 3* bemyndiges vedkommende minister efter forhandling med justitsministeren til – inden for rammerne af databeskyttelsesforordningens artikel 23 – at fastsætte nærmere regler om, at personoplysninger af offentlige myndigheder må viderebehandles til andre formål, end de oprindeligt var indsamlet til, uafhængigt af formålenes forenelighed.

Justitsministeriet vurderer, at bemyndigelsesbestemmelsen i *stk. 3* ligger inden for rammerne af mulighederne for at begrænse bl.a. artikel 5 efter forordningens artikel 23, som i stk. 1, litra e, der bl.a. giver mulighed for at begrænse rettighederne af hensyn til en medlemsstats væsentlige økonomiske interesser.

Det bemærkes, at når pågældende minister udnytter bemyndigelsen i forslagets *stk. 3*, skal bekendtgørelsen leve op til kravene i forordningens artikel 23, stk. 2, hvorefter enhver lovgivningsmæssig foranstaltning, der er omhandlet i artikel 23 stk. 1, som minimum, hvor det er relevant, skal indeholde specifikke bestemmelser vedrørende de i litra a-h angivne krav.

Om disse krav henvises til *betænkningen* side 399-403. Der henvises i øvrigt til afsnit 2.3.1.3. i lovforslagets almindelige bemærkninger.

Det bemærkes for en god ordens skyld, at bestemmelsens *stk. 3* bl.a. kan anvendes til at fastsætte regler om videregivelse af oplysninger fra én myndighed til en anden myndighed.

Til § 6

Det følger af persondatalovens § 6, stk. 1, at behandling af almindelige personoplysninger kun må finde sted, hvis den registrerede har givet sit udtrykkelige samtykke hertil, hvis behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den registrerede er part i, eller af hensyn til at gennemføre foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en sådan aftale, hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, hvis behandlingen er nødvendig for at beskytte den registreredes vitale interesser, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt, eller hvis behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse.

Det er Justitsministeriets vurdering, at der i meget vidt omfang efter databeskyttelsesforordningens artikel 6 vil kunne behandles *almindelige* oplysninger i samme omfang som det er tilfældet i dag efter persondatalovens § 6, stk. 1. Der henvises til afsnit 2.3.2.1. i de almindelige bemærkninger.

I *stk. 1* foreslås det, at der henvises til behandling af almindelige personoplysninger skal ske efter behandlingsbetingelserne i databeskyttelsesforordningens artikel 6, stk. 1, litra a-f, der er direkte anvendelige i Danmark, jf. herved bl.a. *betænkningen* s. 17 ff.

Der henvises til afsnit 2.3.2.2. i de almindelige bemærkninger for nærmere om betingelserne i forordningens artikel 6, stk. 1, litra a-f.

I databeskyttelsesforordningens artikel 8 er der regler om et barns samtykke i forbindelse med informationssamfundstjenester. Der findes ikke tilsvarende regler i persondataloven.

Det fremgår af artikel 8, stk. 1, at hvis artikel 6, stk. 1, litra a, finder anvendelse i forbindelse med udbud af *informationssamfundstjenester* direkte til børn, er behandling af personoplysninger om et barn lovlig, hvis barnet er mindst 16 år, jf. 1. pkt. 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, jf. 2. pkt. Medlemsstaterne kan ved lov fastsætte en lavere aldersgrænse til disse formål, forudsat at en sådan aldersgrænse ikke er under 13 år, jf. 3. pkt.

I *stk. 2* foreslås det at udnytte muligheden i databeskyttelsesforordningens artikel 8, stk. 1, for at fastsætte en lavere aldersgrænse. Aldersgrænsen foreslås at være 13 år.

Der henvises til *betænkningen* s. 185-189.

I *stk. 3* foreslås det, at forordningens artikel 8, stk. 1, 2. pkt., som følge af den foreslåede udnyttelse i *stk. 2* af muligheden for at fastsætte en lavere aldersgrænse gengives – af praktiske og informative grunde – med den konsekvensændring, at den heri nævnte aldersgrænse på 16 år erstattes med en aldersgrænse på 13 år.

Til § 7

Efter databeskyttelsesforordningens artikel 9, stk. 1, gælder der – ligesom efter den gældende persondatalovs § 7, stk. 1 – et forbud mod behandling af oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold. Dog præciseres det som noget nyt i forordningens artikel 9, stk. 1, at forbuddet også gælder for behandling af genetiske data, ligesom det som noget nyt er forbudt efter bestemmelsen at behandle biometriske data med det formål entydigt at identificere en fysisk person.

Efter Justitsministeriets vurdering vil der i meget vidt omfang efter databeskyttelsesforordningens artikel 9, stk. 2, litra a, c, d, e og f, kunne behand-

les oplysninger omfattet af forbuddet i samme omfang, som det er tilfældet i dag efter persondatalovens § 7, stk. 2 og 4. Der henvises til afsnit 2.3.3.1. i de almindelige bemærkninger.

I den foreslåede *stk. 1* henvises der af praktiske og informative grunde til mulighederne for at behandle oplysninger efter databeskyttelsesforordningens undtagelsesbestemmelser i artikel 9, stk. 2, litra a, c, d, e og f, som gælder direkte i Danmark.

Databeskyttelsesforordningens artikel 9, stk. 2, litra b, g, h, i og j, nødvendiggør, at behandlingen er forankret i f.eks. national ret for, at udgangspunktet i artikel 9, stk. 1, om forbud mod behandling af følsomme oplysninger kan fraviges efter disse bestemmelser.

Der henvises til afsnit 2.3.3.2. i de almindelige bemærkninger.

Det følger af persondataloven, at oplysninger om fagforeningsmæssige tilhørsforhold skal kunne ske, hvis behandlingen er nødvendig for overholdelsen af den dataansvarliges arbejdsretlige forpligtelser eller specifikke rettigheder, jf. lovens § 7, stk. 3.

I *stk. 2* foreslås det at videreføre muligheden i persondatalovens § 7, stk. 3, for at behandle oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, med den tilsvarende mulighed herfor i databeskyttelsesforordningens artikel 9, stk. 2, litra b, hvorefter behandling af sådanne oplysninger kan ske, hvis behandling er nødvendig for at overholde den dataansvarliges eller den registreredes arbejdsretlige forpligtelser og specifikke rettigheder.

For nærmere om forordningens artikel 9, stk. 2, litra b, henvises til *betænkningen* s. 211 f.

Efter persondatalovens § 7, stk. 5, gælder forbuddet i lovens § 7, stk. 1, ikke, hvis behandling af følsomme oplysninger er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og hvis behandlingen af oplysningerne foretages af en person, der efter lovgivningen er undergivet tavshedspligt.

I *stk. 3* foreslås det at videreføre muligheden i persondatalovens § 7, stk. 5, for at behandle oplysninger omfattet af databeskyttelsesforordningens arti-

kel 9, stk. 1, hvis behandling af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt jf. databeskyttelsesforordningens artikel 9, stk. 2, litra h.

For nærmere om forordningens artikel 9, stk. 2, litra h, henvises til *betænkningen* s. 218 ff.

Efter persondatalovens § 7, stk. 7, er der mulighed for, at tilsynsmyndigheden kan meddele tilladelse til behandling af følsomme oplysninger omfattet af forbuddet i lovens § 7, stk. 1, af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser. Det overlades til tilsynsmyndigheden at fastsætte nærmere vilkår for behandlingen.

I *stk. 4* foreslås det, at videreføre muligheden i persondatalovens § 7, stk. 7, for, at der kan behandles følsomme oplysninger med tilladelse fra tilsynsmyndigheden (Datatilsynet). Der kan således efter bestemmelsen behandles oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, hvis behandling af oplysninger er nødvendig af hensyn til væsentlige samfundsinteresse, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra g.

Det foreslås, at det ligesom efter persondatalovens § 7, stk. 7, skal være en betingelse for behandling efter denne bestemmelse, at tilsynsmyndigheden (Datatilsynet) har givet tilladelse hertil, dog med den forskel, at kravet om forudgående tilladelse ikke skal gælde for offentlige myndigheder, der behandler oplysninger af hensyn til væsentlige samfundsinteresser.

For nærmere om forordningens artikel 9, stk. 2, litra g, henvises til *betænkningen* s. 216 ff.

Da det kan være vanskeligt på forhånd fuldstændigt at forudse behovet for at kunne behandle personoplysninger omfattet af forordningens artikel 9, stk. 1, foreslås der i *stk. 5* indført en bemyndigelse for vedkommende minister til – efter forhandling med justitsministeren og inden for forordningens rammer – at fastsætte yderligere regler om lovlig behandling af personoplysninger omfattet af forordningens artikel 9, stk. 1.

Fastsættelse af sådanne regler skal ske inden for rammerne af forordningen.

Se nærmere om det nationale råderum i forordningen for at fastsætte yderligere undtagelser til behandlingsforbuddet i artikel 9, stk. 1, i afsnit 2.3.3.2. i de almindelige bemærkninger og *betænkningen* s. 223-233.

Til § 8

Med bestemmelsen foreslås hovedparten af persondatalovens § 8 opretholdt for så vidt angår oplysninger om strafbare forhold.

Der henvises til afsnit 2.3.4.1. i de almindelige bemærkninger.

Bestemmelserne i *stk. 1-2* vedrører den offentlige forvaltning.

I *stk. 1* er det fastsat, at der for den offentlige forvaltning ikke må behandles oplysninger om strafbare forhold, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver.

I *stk. 2* er spørgsmålet om videregivelse af oplysninger om strafbare forhold særligt reguleret. Bestemmelsen omfatter både spørgsmålet om videregivelse til private og spørgsmålet om videregivelse til offentlige myndigheder.

Det bemærkes, at der ikke er fundet behov for at medtage en bestemmelse svarende til persondatalovens § 8, stk. 3. Baggrunden er, at § 8, stk. 3, i dag er blevet udvandet af særlovgivning, der fraviger bestemmelsen, på en lang række områder. Bestemmelsen må derfor anses for at have et yders begrænset anvendelsesområde. Dette skal endvidere ses i lyset af, at persondatalovens § 8 alene foreslås opretholdt for så vidt angår oplysninger om strafbare forhold.

Bestemmelserne i *stk. 3-4* vedrører den private sektor.

I *stk. 3* er det fastsat, at private dataansvarlige må behandle oplysninger om strafbare forhold, hvis den registrerede har givet udtrykkeligt samtykke hertil, jf. *1. pkt.*

Af bestemmelsens 2. *pkt.* følger, at behandling kan ske uden samtykke, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede. Bestemmelsen opstiller meget snævre rammer for, hvornår der kan ske registrering af følsomme personoplysninger uden samtykke. Bestemmelsen giver i lighed med den gældende retstilstand mulighed for, at en virksomhed kan registrere oplysninger om strafbare forhold med henblik på indgivelse af politianmeldelse, f.eks. om butikstyveri, og eventuel senere afgivelse af vidneforklaring i retten. Oplysningerne skal dog destrueres eller lignende snarest muligt, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra e. Bestemmelsen muliggør endvidere, at humanitære organisationer m.v., såsom Amnesty International, uden den pågældendes samtykke kan behandle oplysninger om strafbare forhold, f.eks. fordi den registrerede ikke kan findes, eller fordi det ikke har været muligt at rette henvendelse til den pågældende som følge af fængsling eller lignende.

I *stk. 4* er spørgsmålet om privates videregivelse af oplysninger om strafbare forhold særligt reguleret.

Af bestemmelsens 1. *pkt.* følger således, at de i *stk. 3* nævnte oplysninger om strafbare forhold ikke må videregives uden den registreredes samtykke.

Videregivelse kan dog ske uden samtykke, når videregivelsen sker til varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrundes hemmeligholdelse, jf. 2. *pkt.*

Bestemmelsen i *stk. 5* vedrører de tilfælde, hvor betingelserne i databeskyttelsesforordningens artikel 9, stk. 2, og/eller den foreslåede § 7 ville være opfyldt, hvis oplysninger om strafbare forhold var omfattet af forbudet i artikel 9, stk. 1.

Det foreslås i bestemmelsen, at oplysninger om strafbare forhold ud over de tilfælde, der er nævnt i *stk. 1-4*, skal kunne behandles, hvis betingelserne i den foreslåede § 7 er opfyldt.

Til § 9

I bestemmelsen fastsættes særlige regler for behandling af oplysninger med henblik på at føre et retsinformationssystem.

Bestemmelsen i forslaget § 9 svarer til persondatalovens § 9. Den gældende praksis på området vil dermed fortsat være af betydning. Databeskyttelsesforordningen indeholder regler, som i vidt omfang svarer til reglerne i databeskyttelsesdirektivets artikel 8, stk. 4, som persondatalovens § 9 har sin baggrund i. Justitsministeriet finder derfor, at der på samme måde som i dag kan fastsættes særlige regler for behandling af oplysninger med henblik på at føre et retsinformationssystem.

Der henvises i øvrigt til *betænkningen* side 256-261.

Bestemmelsen i *stk. 1* indebærer, at oplysninger, der er omfattet af databeskyttelsesforordningens artikel 9, stk. 1, og 10 kan behandles med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning. Dette vil navnlig være systemer, som er til rådighed for en bredere kreds af abonnenter for at sikre en ensartet retsanvendelse. Derimod vil en myndigheds eller virksomheds interne retsinformationssystem være underlagt de almindelige behandlingsregler.

Efter bestemmelsen skal behandlingen være nødvendig for førelsen af systemerne. Dette betyder, at bestemmelsen ikke hjemler adgang til at behandle oplysninger i et retsinformationssystem, hvis systemet kunne tjene sit formål ligeså sikkert og effektivt uden oplysninger om enkeltpersoner.

Det følger af bestemmelsen i *stk. 2*, at der ikke senere må ske behandling af oplysninger, som er omfattet af stk. 1, til andre formål. Dette medfører bl.a., at oplysningerne ikke må anvendes til at træffe foranstaltninger eller afgørelser vedrørende registrerede personer. Dette gælder også med hensyn til behandling af andre oplysninger, som i henhold til databeskyttelsesforordningens artikel 6 alene foretages med henblik på at føre retsinformationssystemer. Oplysningerne må naturligvis anvendes i forbindelse med f.eks. førelse af en retssag, idet en sådan anvendelse ikke ligger uden for formålet med et retsinformationssystem.

Med *stk. 3* sikres det, at der - ligesom hvad der i dag gælder for private retsinformationssystemer - kan fastsættes vilkår for behandling af de i stk. 1 nævnte oplysninger. Herudover kan tilsynsmyndigheden efter bestemmelsen meddele nærmere vilkår for den behandling af de i forordningens artikel 6 nævnte oplysninger, som alene sker i tilknytning til førelsen

af retsinformationssystemer. Der kan f.eks. fastsættes vilkår om, at personnavne, præcise adresseangivelser og eventuelt andre identifikationsoplysninger fjernes i samme omfang, som dette skal ske efter Justitsministeriets cirkulære nr. 85 af 8. juli 1988 om indlæggelse af afgørelser i Retsinformation.

Til § 10

I bestemmelsen videreføres persondatalovens § 10 tilpasset databeskyttelsesforordningens rammer. Bestemmelsen fastsættes inden for rammerne af databeskyttelsesforordningens artikel 9, stk. 2, litra j, hvorefter behandling af følsomme oplysninger omfattet af artikel 9, stk. 1, er lovlig, bl.a. hvis behandling er nødvendig 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 væsentligst indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Efter bestemmelsen i stk. 1 vil der kunne behandles oplysninger som nævnt i databeskyttelsesforordningens artikel 9, stk. 1, og artikel 10, såfremt behandlingen alene finder sted med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning. Det forudsættes, at der ikke sker nogen indskrænkning i forhold til de muligheder, som dataansvarlige har for at foretage undersøgelser i statistisk eller videnskabeligt øjemed efter den gældende persondatalov. Såfremt en behandling tillige har andre formål, vil behandlingen skulle vurderes efter bestemmelserne i databeskyttelsesforordningens artikel 9, stk. 2, og artikel 10. Bestemmelsen finder kun anvendelse, hvis behandlingen er nødvendig for udførelsen af statistiske eller videnskabelige undersøgelser.

Det følger af stk. 2, at der ikke senere må ske behandling af oplysninger, som er omfattet af stk. 1, til andre formål. Dette medfører bl.a., at oplysningerne ikke må anvendes til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer. Der vil således alene kunne ske efterfølgende behandling, herunder videregivelse, efter stk. 3 og 4, jf. herom nedenfor. Tilsvarende gælder med hensyn til behandling af andre oplysninger, som i henhold til § 6 alene foretages med henblik på at udføre statistiske eller videnskabelige undersøgelser.

Bestemmelsen i stk. 3 fastsætter endelig, at videregivelse til tredjemand kun kan ske efter forudgående tilladelse fra vedkommende tilsynsmyndighed og i givet fald kun med henblik på udførelse af undersøgelser i statistisk eller videnskabeligt øjemed, jf. stk. 1 og 2. Efter bestemmelsen kan vedkommende tilsynsmyndighed meddele vilkår til sikring af, at oplysningerne alene vil blive anvendt til statistiske eller videnskabelige formål samt vilkår til beskyttelse af de registreredes privatliv.

Efter den foreslåede bestemmelse videreføres det således, at vedkommende tilsynsmyndighed kan give en generel tilladelse til videregivelsen. Det skal i tilladelsen præciseres, hvilke oplysningstyper der må videregives. Endvidere skal det anføres, til hvilke undersøgelser og i hvilken periode videregivelse må finde sted. Tilladelsen vil f.eks. kunne gives i forbindelse med anmeldelsen af en behandling, hvis den dataansvarlige allerede på anmeldelsestidspunktet kan forudse, at en videregivelse til tredjemand til brug for statistiske eller videnskabelige undersøgelser vil blive aktuel.

Der henvises til *betænkningen* bl.a. side 102ff, s. 222f og side 982-990.

Det foreslås i *stk. 4* at bemyndige sundhedsministeren til efter forhandling med justitsministeren – og uanset udgangspunktet i stk. 2 – at fastsætte regler om, at oplysninger omfattet af databeskyttelsesforordningens artikel 6 og 9, som er behandlet med henblik på at udføre sundhedsvidenskabelig forskning og statistik senere kan behandles til andre formål end videnskabelige eller statistiske formål, hvis en sådan behandling er nødvendig til varetagelse af den registreredes vitale interesser.

Det er hensigten at udmønte bemyndigelsen ved at fastsætte regler, der tillader behandling af sådanne personoplysninger i situationer, hvor der i forbindelse med sundhedsvidenskabelige forskningsprojekter og sundhedsvidenskabelige statistiske undersøgelser fremkommer oplysninger om, at den registrerede lider af livstruende eller klart alvorlig sygdom, som enten kan behandles, forebygges eller lindres, og det derfor er nødvendigt af hensyn til den registreredes vitale interesser at behandle, herunder videregive, oplysningerne med henblik på dels at informere den registrerede om dette fund, dels at benytte oplysningerne til at vurdere, om og i givet fald hvilken patientbehandling som bør iværksættes.

Der vil ved fastsættelsen af regler om behandling af oplysninger i forbindelse håndtering af sådanne fund blive stillet krav om, at der enten skal

foreligge et samtykke fra den registrerede (afgivet inden forskningsprojektets påbegyndelse) eller på anden vis være passende foranstaltninger, der sikrer den registreredes interesser og understøtter individbeskyttelse og selvbestemmelse, herunder retten til ikke at vide (f.eks. høring af sagkyndig komité).

Bemyndigelsen vil ligeledes kunne blive benyttet til at fastsætte regler, der tillader behandling af sådanne oplysninger i situationer, hvor behandlingen vil være nødvendig af hensyn til varetagelse af den registreredes vitale interesser i forbindelse med valg af konkret patientbehandling, dvs. hvor behandling af oplysningerne sker som beslutningsstøtte for en sundhedspersons beslutning om konkret – skræddersyet – patientbehandling (personlig medicin) til patienter, som lider af livstruende sygdomme, som kan behandles, forebygges eller lindres.

Der vil ved fastsættelsen af regler om behandling af oplysninger til beslutningsstøtte blive stillet krav om, at der altid skal foreligge et samtykke fra den registrerede.

Der vil endvidere blive fastsat regler om, at det alene vil være personer, som er omfattet af en lovbestemt tavshedspligt, herunder f.eks. sundhedspersoner, som er omfattet af tavshedspligt, jf. sundhedslovens § 40, der kan videregive oplysninger om livstruende eller klart alvorlige sygdomme til den registrerede. Hvis den pågældende forsker ikke selv er omfattet af en lovbestemt tavshedspligt, vil videregivelsen af de omhandlede oplysninger til den registrerede således skulle ske via en sundhedsperson.

Det bemærkes, at det kan komme på tale på et senere tidspunkt at fastsætte bestemmelser om, at oplysninger, der stammer fra sundhedsvidenskabelige statistiske undersøgelser, ligeledes vil kunne behandles med henblik på varetagelse af den registreredes vitale interesser, fx statistik, der bruges til patientsikkerhedsformål, monitorering mv.

Muligheden for at fastsætte nationale særregler, som muliggør videre behandling til brug for andre formål end videnskabelige og historiske forskningsformål og statistiske formål vurderes at holde sig inden for rammerne af databeskyttelsesforordningens artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j.

Der henvises til *betænkningen* side 984 ff.

Til § 11

I bestemmelsen fastsættes regler for, i hvilket omfang offentlige myndigheder og private kan behandle oplysninger om personnumre.

Bestemmelsen i forslagets § 11 svarer til persondatalovens § 11. Den gældende praksis på området vil dermed fortsat være af betydning.

Af bestemmelsens *stk. 1* følger, at offentlige myndigheder vil kunne behandle oplysninger om personnumre med henblik på en entydig identifikation samt som journalnummer. Bestemmelsen indebærer, at der vil kunne ske behandling af oplysninger om personnumre i samme omfang som efter den gældende persondatalov.

Bestemmelsen indebærer, at en forvaltningsmyndighed ikke må føre åbne postlister, hvor borgernes personnumre er anvendt som journalnummer.

I bestemmelsens *stk. 2* fastsættes regler for privates behandling af oplysninger om personnumre.

Efter reglen i *nr. 1* vil private virksomheder m.v. kunne foretage behandling, herunder registrering og videregivelse, af oplysninger om personnumre, såfremt det følger af lov eller bestemmelser fastsat i henhold til lov. Dette svarer til den gældende ordning i persondataloven, jf. lovens § 11, stk. 2, nr. 1.

Herudover vil der efter bestemmelsen kunne ske behandling af oplysninger om personnumre, hvis den registrerede har givet sit samtykke hertil i overensstemmelse med databeskyttelsesforordningens artikel 7, jf. *nr. 2*. Om samtykkekravet henvises i øvrigt til databeskyttelsesforordningens artikel 4, nr. 11.

Endelig vil der efter bestemmelsen *nr. 3* kunne ske behandling uden samtykke, hvis dette alene sker i forbindelse med undersøgelser i videnskabeligt eller statistisk øjemed. Hermed videreføres den gældende retstilstand vedrørende registrering og videregivelse af personnumre som led i udførelsen af forskning eller statistik.

Bestemmelsen indebærer endvidere, at registrerede oplysninger om personnumre kan *videregives* i samme omfang som efter den hidtil gældende retstilstand i persondatalovens § 11, stk. 2, nr. 3. Dette giver navnlig mu-

lighed for at opretholde den nuværende adgang til – på grundlag af kundernes personnumre – at foretage samkøring i den finansielle sektor.

Med den foreslåede bestemmelse tilsigtes i øvrigt ikke at indskrænke adgangen til at anvende oplysninger om personnumre, som er registreret med særlig lovhjemmel, jf. § 11, stk. 2, nr. 1.

Det bemærkes, at kreditoplysningsbureauers publikationer ikke må indeholde oplysninger om de registreredes personnummer, jf. lovforslagets § 21, stk. 2, 2. pkt., der opretholder den gældende bestemmelse i persondatalovens § 23, stk. 2, 2. pkt.

Af bestemmelsens *stk. 3* følger, at private dataansvarliges behandling af oplysninger om personnumre i henhold til bestemmelsen i *stk. 2, nr. 3*, ikke må indebære, at der sker offentliggørelse af oplysningerne uden den registreredes udtrykkelige samtykke. Herved sikres det, at oplysninger, som lovligt kan behandles efter *stk. 2, nr. 3*, ikke uden den berørtes accept kan videregives til en bredere kreds af personer. Det bemærkes, at det for så vidt angår behandling af oplysninger om personnumre i medfør af bestemmelsen i *stk. 2, nr. 2*, forudsættes, at offentliggørelse kun vil kunne ske, hvis den registrerede udtrykkeligt har meddelt samtykke hertil.

For så vidt angår bestemmelsens *stk. 4*, finder Justitsministeriet, at private – i modsætning til i dag – bør have mulighed for at behandle oplysninger om personnumre, når betingelserne i forslagets § 7 er opfyldt. Der kan i den forbindelse bl.a. henvises til, at der stilles skærpede krav til behandlingsgrundlag i forslagets § 7 om følsomme oplysninger. I tilfælde, hvor de skærpede betingelser for at behandle følsomme oplysninger er opfyldt vil der derfor være formodning for, at hensynet til integritet mv. er tilstrækkeligt varetaget også i relation til behandling af oplysninger om personnumre.

Dette skal ses i lyset af, at oplysninger om personnumre også skal kunne behandles, hvis de særlige betingelser i forslagets § 7 er opfyldt.

Af bestemmelsens *stk. 2, nr. 4*, fremgår således, at private også kan behandle oplysninger om personnumre, når betingelserne i forslagets § 7 er opfyldt.

Med lovforslagets § 12 er det hensigten at bringe fuldstændig sikkerhed for, at der på det offentlige og private arbejdsmarked lovligt kan behandles personoplysninger før, under og efter ansættelsesforholdet i samme omfang som hidtil.

Lovforslagets § 12 er tiltænkt som en *supplerende* hjemmelsbestemmelse, hvorefter der i ansættelsesforhold *også* kan behandles personoplysninger.

Der kan således fortsat behandles personoplysninger i ansættelsesforhold indenfor rammerne af lovforslagets øvrige behandlingsregler, herunder §§ 6-8, og forordningens behandlingsregler i artikel 6, 9 og 10.

Der kan i den forbindelse særligt henvises til det anførte i *betænkningen* side 139-141, hvoraf det fremgår, at offentlige myndigheder – i lyset af, at forordningens artikel 6, stk. 1, litra f, 2. afsnit, ikke, som led i udførelsen af deres opgaver kan foretage lovlig behandling af hensyn til at forfølge en legitim interesse – fremover må kunne anvende artikel 6, stk. 1, litra e, om ”en opgave i samfundet interesse” som behandlingshjemmel, når, når de behandler personoplysninger som arbejdsgiver.

Al behandling af personoplysninger, også i ansættelsesforhold, skal også leve op til de grundlæggende principper i forordningens artikel 5.

Lovforslagets § 12 omhandler almindelige oplysninger omfattet af forordningens artikel 6 og de følsomme oplysninger omfattet af forordningens artikel 9, jf. lovforslagets §§ 6-7. Lovforslagets § 12 omhandler således ikke oplysninger om strafbare forhold omfattet af forordningens artikel 10. Der henvises her i stedet til lovforslagets § 8. For så vidt angår arbejdsgivers behandling af oplysninger om strafbare forhold, f.eks. i en straffeattest, er dette således reguleret i de forskellige stykker i lovforslagets § 8 alt efter, om der er tale om offentlige eller private arbejdsgivere, jf. også *betænkningen* side 972.

Med forslaget til *stk. 1* foreslås det, at behandling af personoplysninger omfattet af artikel 6, stk. 1, og artikel 9, stk. 1, i databeskyttelsesforordningen kan finde sted, hvis behandlingen er nødvendig for at overholde den dataansvarliges eller den registreredes *arbejdsretlige forpligtelser* eller *rettigheder*, som fastlagt i anden lovgivning eller kollektive overenskomster.

Ordlyden af stk. 1 lægger sig helt om ad forordningens artikel 9, stk. 2, litra b, og med bestemmelsen slås det således helt fast, at både oplysninger omfattet af artikel 6, stk. 1, og af artikel 9, stk. 1, kan behandles efter samme bestemmelse, nemlig lovforslagets § 12, stk. 1, når der foreligger en arbejdsretlig forpligtelse eller rettighed.

Med forslaget til *stk. 2* foreslås det, at behandling af oplysninger som nævnt i stk. 1 også må finde sted, hvis behandlingen er nødvendig for, at den dataansvarlige kan forfølge en legitim interesse, som *udspringer* af anden lovgivning eller kollektive overenskomster, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, går forud herfor.

Der foregår i dag ofte behandling af personoplysninger i ansættelsesforhold lovligt på baggrund af interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7, selvom behandlingen ikke nødvendiggjort af en arbejdsretlig *forpligtelse*, men som på anden vis har sin baggrund i f.eks. en kollektiv overenskomst. Sådan behandling kan forsætte på baggrund af denne foreslåede interesseafvejningsregel i stk. 2, der svarer reglen i forordningens artikel 6, stk. 1, litra f. Med den foreslåede bestemmelse sikres der i øvrigt, at en sådan afvejningsregel kan anvendes også i forbindelse med ansættelsesforhold i det offentlige, selvom det af forordningens artikel 6, stk. 1, litra f, 2. afsnit, fremgår, at interesseafvejningsreglen ikke gælder for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

Med forslaget til *stk. 3* er det hensigten, at slå helt fast, at samtykke også kan anvendes som behandlingsgrundlag før, under og efter ansættelse. Der henvises til *betænkningen* s. 183.

Til § 13

I persondatalovens § 6, stk. 2-4, er der nærmere betingelser for behandling af personoplysninger i forbindelse med markedsføring. I persondatalovens § 12 er der endvidere fastsat markedsføringsregler vedrørende adresserings- og kuverteringsbureauer. Der henvises til afsnit 2.3.9. i de almindelige bemærkninger. Desuden er der i persondatalovens § 36, stk. 2, 1. pkt., fastsat regler om pligtmæssig undersøgelse i CPR af, om de registrerede frabeder sig henvendelser i markedsføringsøjemed forinden videregivelse eller anvendelse af oplysningerne i markedsføringsøjemed. Der henvises til afsnit 2.3.9. i de almindelige bemærkninger.

Det foreslås i § 13, at videreføre bestemmelserne i persondatalovens § 6, stk. 2-4, og § 12. Endvidere foreslås det at videreføre persondatalovens § 36, stk. 2, 1. pkt., tilpasset databeskyttelsesforordningens ændringer af indsigelsesretten i forhold til markedsføring.

I den foreslåede *stk. 1* fastsættes hovedreglen om, at virksomheder ikke må videregive oplysninger om forbrugere til andre virksomheder i markedsføringsøjemed (eller anvende oplysningerne på vegne af andre virksomheder i markedsføringsøjemed), medmindre forbrugeren har givet sit udtrykkelige samtykke til det. Om samtykkekravet henvises til databeskyttelsesforordningens artikel 4, nr. 11.

I *stk. 2* angives de tilfælde, hvor der gøres undtagelse fra kravet om samtykke i stk. 1. Som det fremgår af bestemmelsen, kan kundeoplysninger kun videregives uden kundens samtykke, hvis to betingelser er opfyldt.

For det første skal der være tale om generelle kundeoplysninger, der danner grundlag for inddeling i kundekategorier.

Er denne betingelse opfyldt, skal videregivelsen for det andet følge af den interesseafvejning, som er fastsat i databeskyttelsesforordningens artikel 6, stk. 1, litra f. Efter denne bestemmelse kan videregivelse ske, hvis videregivelse 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.« Med dette supplerende krav sikres det, at videregivelse af generelle kundeoplysninger i markedsføringsøjemed ikke kan ske, hvis interesseafvejningen undtagelsesvis måtte tale herimod. Som eksempel herpå kan nævnes den situation, at en virksomhed har orienteret sine kunder om, at den ikke vil videregive oplysninger om kunderne til andre virksomheder til brug for markedsføring. Hvis virksomheden på trods heraf alligevel skulle beslutte sig for at videregive oplysningerne, vil hensynet til kunderne, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra f, efter omstændighederne kunne tale imod, at en sådan videregivelse kan ske uden kundernes forudgående samtykke.

Som eksempler på oplysninger, der herefter vil kunne videregives uden samtykke efter den foreslåede bestemmelse, kan nævnes oplysninger om kundens navn, adresse, køn og alder. Det samme gælder generelle oplys-

ninger om f.eks., at kunden er husejer, bilejer, computerejer og lignende. Tilsvarende gælder f.eks. oplysninger om, at der er tale om en kunde til fritidsartikler, til baby- og småbørnsartikler, til økologiske varer, til vin- og spiritus eller andre generelt afgrænsede varegrupper.

Derimod vil det efter den foreslåede bestemmelse ikke være muligt uden samtykke at videregive oplysninger, som afslører følsomme oplysninger om kunden.

Det vil heller ikke være muligt at videregive mere detaljerede kundeoplysninger eller forbrugsvaner uden kundens samtykke. Der må således f.eks. ikke videregives oplysninger om, hvorvidt kundens bil er købt på kredit, og i givet fald oplysninger om vilkårene for kreditten. Der må heller ikke videregives oplysninger om, hvilken mængde vin kunden køber. Det gælder, selv om dette ikke i sig selv afslører, at kunden har et spiritusmisbrug. Der må heller ikke videregives mere detaljerede oplysninger om, hvilken slags vin kunden køber.

Kan videregivelse efter det anførte ske uden kundens samtykke, følger det herudover af databeskyttelsesforordningens artikel 21, stk. 3, at videregivelse ikke må finde sted med henblik på direkte markedsføring, hvis kunden har gjort indsigelse imod det.

I *stk. 3* angives det for at undgå enhver tvivl herom udtrykkeligt, at der ikke uden forbrugerens samtykke må videregives følsomme oplysninger om forbrugeren til andre virksomheder til brug ved markedsføring.

Det angives endvidere i bestemmelsen, at justitsministeren ved bekendtgørelse vil kunne begrænse adgangen til efter *stk. 2* at videregive andre typer af oplysninger til brug ved markedsføring. Baggrunden for bestemmelsen er, at det ikke på forhånd kan udelukkes, at der vil kunne vise sig et behov for, at visse typer oplysninger, ikke skal kunne videregives uden forbrugers udtrykkelige samtykke.

I *stk. 4* angives det, at en virksomhed – hver gang den ønsker at videregive kundeoplysninger til andre virksomheder til brug ved direkte markedsføring – skal tjekke i CPR, om kunden har frabedt sig henvendelser i markedsføringsøjemed. I bekræftende fald må oplysningerne ikke videregives til dette formål, jf. databeskyttelsesforordningens artikel 21, stk. 3.

For så vidt angår den registrerede kunde eller lignende, der ikke i CPR har frabedt sig henvendelser i markedsføringsøjemed, skal virksomheden endvidere – senest på tidspunktet for den første kommunikation med den registrerede – efter databeskyttelsesforordningens artikel 21, stk. 4, udtrykkeligt gøre den registrerede opmærksom på retten til at gøre indsigelse efter forordningens artikel 21, stk. 2, mod behandling af personoplysninger til direkte markedsføring.

Reglerne gælder også i den situation, hvor oplysningerne anvendes på vegne af en anden virksomhed med henblik på direkte markedsføring.

Bestemmelsen beskriver således den fremgangsmåde, som den dataansvarlige virksomhed skal følge for at sikre sig, at forbrugeren ikke har gjort indsigelse imod, at generelle kundeoplysninger om den pågældende videre gives til en anden virksomhed med henblik på direkte markedsføring.

Fremgangsmåden skal også følges i tilfælde, hvor den dataansvarlige virksomhed ikke ønsker at videregive oplysningerne til en anden virksomhed, men derimod selv at anvende oplysningerne på vegne af en anden virksomhed med henblik på direkte markedsføring.

Efter bestemmelsen skal den dataansvarlige virksomhed undersøge i CPR, om forbrugeren har frabedt sig henvendelser i markedsføringsøjemed.

Af bestemmelsen i *stk. 5* fremgår, hvilke oplysninger en dataansvarlig, som med henblik på markedsføring sælger adresser over grupper af personer, eller som for tredjemand foretager kuvertering eller udsendelse af meddelelser til sådanne grupper, må behandle. Bestemmelsen omfatter således kun de situationer, hvor bureauet er dataansvarlig for de oplysninger, som sælges eller danner grundlag for kuvertering eller udsendelse for tredjemand. Hvis en dataansvarlig derimod overlader egne oplysninger til et bureau med henblik på, at bureauet foretager kuvertering eller udsendelse, er det de almindelige behandlingsbestemmelser samt bestemmelserne i databeskyttelsesforordningens artikel 21, stk. 2 og 3, om indsigelse imod behandling med henblik på direkte markedsføring, som finder anvendelse. I så fald vil bureauet blot være databehandler og må derfor ikke behandle oplysningerne til andre formål end dem, som den dataansvarlige giver instruks om, jf. databeskyttelsesforordningens artikel 29, sammenholdt med artikel 4, nr. 8.

Af reglen i *nr. 1* følger, at der må behandles oplysninger om navn, adresse, stilling, erhverv, e-postadresse og telefon- og telefaxnummer. Endvidere må oplysninger, der indgår i erhvervsregistre, som i henhold til lov eller bestemmelser fastsat i henhold til lov er beregnet til at informere offentligheden, behandles, jf. *nr. 2*. Endelig må andre oplysninger behandles, hvis den registrerede har givet udtrykkeligt samtykke dertil, jf. *nr. 3*. Et sådant samtykke skal opfylde de betingelser, som fremgår af databeskyttelsesforordningens artikel 4, nr. 11. Et samtykke skal endvidere indhentes i overensstemmelse med reglerne i markedsføringslovens § 10.

Adgangen til efter bestemmelsen at behandle de i nr. 1-3 nævnte oplysninger gælder dog ikke, hvis dette vil være i strid med bestemmelsen i *stk. 5*. Af denne bestemmelses *1. pkt.* fremgår, at der ikke må ske behandling af følsomme oplysninger. Dette gælder, uanset om der er givet samtykke dertil. Efter bestemmelsens *2. pkt.* kan justitsministeren fastsætte yderligere begrænsninger i adgangen til at behandle bestemte typer af oplysninger.

Det bemærkes, at den registrerede altid vil kunne fremsætte indsigelse mod, at et dataansvarligt adresserings- og kuverteringsbureau behandler oplysninger om den pågældende med henblik på direkte markedsføring, herunder salg, kuvertering eller udsendelse, jf. databeskyttelsesforordningens artikel 21, stk. 2, ligesom adresserings- og kuverteringsbureauet skal følge proceduren i forordningens artikel 21, stk. 3.

I de tilfælde, hvor videregivelse af oplysninger til en anden virksomhed eller anvendelse af oplysninger på vegne af en anden virksomhed med henblik på direkte markedsføring over for den registrerede kan ske uden samtykke efter reglerne i lovforslagets § 13, stk. 1-3, foreslås det, at virksomheden (den dataansvarlige) skal iagttage proceduren i stk. 4, og databeskyttelsesforordningens artikel 21.

Det betyder, at virksomheden ikke må videregive oplysninger om en kunde til andre virksomheder med henblik på direkte markedsføring, hvis kunden har gjort indsigelse herimod.

I *stk. 6* angives det for at undgå enhver tvivl herom udtrykkeligt, at behandling af oplysninger omfattet af stk. 4 ikke må omfatte følsomme oplysninger.

Det angives endvidere i bestemmelsen, at justitsministeren ved bekendtgørelse vil kunne begrænse adgangen til efter stk. 4 at behandle andre typer

af oplysninger. Baggrunden for bestemmelsen er, at det ikke på forhånd kan udelukkes, at der vil kunne vise sig et behov for, at visse typer oplysninger ikke skal kunne behandles.

Til § 14

Bestemmelsen i forslaget § 14 svarer til persondatalovens § 14. Den gældende praksis på området vil dermed fortsat være af betydning.

Bestemmelsen regulerer spørgsmålet om arkivering. Efter bestemmelsen kan oplysninger, som er omfattet af loven, overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen. Bestemmelsen indebærer, at der vil kunne ske arkivering af behandlede oplysninger i det omfang, dette følger af reglerne i arkivlovgivningen. Dette gælder for oplysninger, som er behandlet for såvel offentlige myndigheder som for private.

Der henvises i øvrigt til *betænkningen* side 990-995.

Til kapitel 4

Videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige

Til § 15

Efter *stk. 1* kan oplysninger om gæld til det offentlige videregives til kreditoplysningsbureauer efter reglerne i lovens kapitel 4.

Bestemmelserne i kapitlet omfatter kreditoplysningsbureauvirksomhed, hvorved forstås virksomhed med behandling af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse (kreditoplysningsbureau).

Bestemmelsen svarer til persondatalovens § 15. Den gældende praksis på området vil dermed fortsat være af betydning.

Efter lovforslaget skal offentlige myndigheder ikke være forpligtede til at videregive de omhandlede oplysninger til kreditoplysningsbureauer. Med

forslaget søges alene tilvejebragt en mulighed herfor, som kan udnyttes, såfremt det på et givet område må anses for hensigtsmæssigt.

Baggrunden herfor er, at det må være den enkelte myndighed, der bedst kan vurdere, om en udnyttelse af muligheden for at videregive de pågældende oplysninger vil have den ønskede restanceinddrivelseseffekt.

Det forudsættes, at en myndigheds beslutning om videregivelse af oplysninger om gæld ikke er en afgørelse i forvaltningslovens forstand, men derimod et led i myndighedens faktiske forvaltningsvirksomhed.

Dette indebærer bl.a., at selve beslutningen om videregivelsen ikke vil kunne indbringes for den eventuelle særlige administrative rekursmyndighed, som den videregivende myndigheds afgørelser i øvrigt måtte være undergivet.

Klage over den videregivende myndigheds virksomhed – herunder videregivelse af oplysninger om gældsforhold – vil derimod i sædvanligt omfang kunne indgives til en overordnet myndighed i henhold til en almindelig ulovbestemt adgang til at klage inden for over-/underordnelsesforhold.

Mere generelt skal myndigheder i øvrigt under udøvelsen af deres virksomhed iagttage den almindelige forvaltningsretlige lighedsgrundsætning, hvilket vil sige, at en myndighed skal behandle lige tilfælde ens – eller udtrykt på en anden måde – en myndighed skal sagligt kunne begrunde en eventuel forskelsbehandling af borgerne.

Denne lighedsgrundsætning vil også skulle iagttages af myndighederne i forbindelse med videregivelse af oplysninger om gæld til kreditoplysningsbureauer.

Lighedsgrundsætningen er imidlertid ikke til hinder for, at der fastsættes og følges forskellige regler fra et myndighedsområde til et andet afhængig af de pågældende myndigheders virksomhed.

Omfattet af udtrykket »oplysninger om gæld« i stk. 1 er elektronisk registrerede oplysninger om skyldnerens identitet (eksempelvis navn, adresse og telefonnummer samt fødselsdato og år) og gældens størrelse. Det er disse oplysninger om kreditors identitet, som kan videregives. Der skal derimod ikke kunne videregives oplysninger om gældens art, f.eks. om gælden udspringer af et krav efter sociallovgivningen.

Ved »gæld« forstås en gæld, der udspringer af et konkret retsforhold, der vedrører en bestemt form for ydelse, betaling mv.

Således vil manglende betaling af en løbende ydelse – som f.eks. daginstitutionsbetaling – udgøre en samlet gæld i forslagets forstand, uanset at gælden f.eks. vedrører betaling for mere end et barn og i flere perioder.

På tilsvarende måde vil skatte- og afgiftskrav skulle ses under et, for så vidt der er tale om samme inddrivelsesmyndighed, uanset om kravene udspringer fra forskellige indtægter, dispositioner mv. og/eller er påløbet i forskellige tidsrum.

Der er ikke noget til hinder for, at der videregives oplysninger om flere krav, i det omfang kravene hver for sig opfylder betingelserne for videregivelse herunder beløbsgrænsen.

Det følger af *stk. 2*, at oplysninger som nævnt i databeskyttelsesforordningens artikel 9, stk. 1, eller artikel 10 ikke må videregives. Uanset, at den omhandlede videregivelse som udgangspunkt ikke vil indebære en videregivelse af oplysninger af denne karakter, er det fundet hensigtsmæssigt udtrykkeligt at medtage en bestemmelse herom.

En tilsvarende regel findes i persondatalovens § 15, stk. 2. Den gældende praksis på området vil dermed fortsat være af betydning.

Den omstændighed, at en offentlig myndighed til en videre kreds videregiver fortrolige oplysninger, kan efter omstændighederne bevirke, at oplysningerne mister deres fortrolige karakter (bliver offentligt tilgængelige), hvilket ligeledes kan få indflydelse på afgørelsen af spørgsmål om aktindsigt.

Det er uheldigt, såfremt en myndigheds videregivelse af oplysninger fra registre efter bestemmelserne i forslaget skulle medføre en videre adgang til for enhver at kræve aktindsigt i dokumenter indeholdende de pågældende oplysninger. Hertil kommer, at der med en videregivelse efter forslagets bestemmelser er tale om en videregivelse til en lukket kreds bestående af kreditoplysningsbureauet og dets abonnenter, i det omfang disse forespørger på den pågældende person. Abonnenterne er kontraktligt forpligtet til at hemmeligholde de modtagne oplysninger.

Det er derfor fundet hensigtsmæssigt og rimeligt at opretholde en bestemmelse i lovforslagets *stk. 3*, hvor det udtrykkeligt fastslås, at fortrolige oplysninger videregivet efter reglerne i det foreslåede kapitel 4 ikke bliver offentligt tilgængelige i øvrigt. Oplysningerne mister således ikke af den grund deres fortrolige karakter, ligesom videregivelsen ikke har betydning for afgørelsen af spørgsmål om aktindsigt med hensyn til de pågældende oplysninger.

Det kan hertil tilføjes, at kreditoplysningsbureauerne heller ikke offentliggør oplysningerne, men alene videregiver til abonnenter og under iagttagelse af vilkår om, hvad der kan begrunde opslag.

Bestemmelsen i *stk. 3* svarer til persondatalovens § 15, *stk. 3*. Den gældende praksis på området vil dermed fortsat være af betydning.

Der henvises til Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, side 63-65 og 277-282.

Til § 16

Lovforslagets *stk. 1* indeholder de nærmere betingelser for, hvornår en myndighed må videregive oplysninger om gæld til et kreditoplysningsbureau. Bestemmelsen er ikke til hinder for, at den enkelte minister og eventuelt den enkelte myndighed efter de foreslåede regler herom fastsætter yderligere eller skærpede betingelser for videregivelsen. Bestemmelsen har således karakter af en minimumsregel.

Bestemmelsen i forslaget § 16 svarer til persondatalovens § 16. Den gældende praksis på området vil dermed fortsat være af betydning.

Efter *stk. 1, nr. 1*, kan der for det første ske videregivelse, hvis det følger af lov eller bestemmelser fastsat i henhold til lov. Det er fundet hensigtsmæssigt udtrykkeligt at opretholde denne videregivelsesmulighed, der først og fremmest vil få betydning indenfor områder, hvor der hovedsageligt er tale om fordringer, der ikke opfylder beløbsgrænsen på 7.500 kr., men hvor man uanset dette finder, at der skal være mulighed for at benytte kreditoplysningsbureauer. Det bemærkes, at forslaget øvrige bestemmelser tillige finder anvendelse for så vidt angår videregivelse efter sådanne særligt fastsatte bestemmelser, i det omfang andet ikke er bestemt.

Efter *stk. 1, nr. 2*, kan der for det andet ske videregivelse, hvis den samlede gæld er forfalden og overstiger 7.500 kr.

Det er således – udover beløbskravet – også en betingelse for videregivelse, at gælden er forfalden. Forfaldstiden er det tidspunkt, på hvilket fordringshaveren kan kræve betaling.

Hvis der er bevilget henstand eller indgået en aftale om afdragsvis betaling, og denne aftale overholdes, kan videregivelse af oplysninger om gælden ikke ske. Formålet med denne begrænsning er at tilskynde til betaling af gælden, herunder afdragsvis betaling af gælden. Derimod forhindrer den omstændighed, at forhandlinger om en afdragsaftale er indledt inden videregivelsen, ikke, at oplysninger om gælden kan videregives. I sådanne tilfælde, særligt hvor myndigheden skønner, at aftalen vil kunne indgås inden for kort tid, vil det dog ofte være hensigtsmæssigt at udskyde beslutningen om at videregive de pågældende oplysninger.

Den omstændighed, at skyldneren inden videregivelsen af oplysningerne har indgivet klage over kravets eksistens eller størrelse, er ikke til hinder for videregivelsen, i det omfang kravet er eksigibelt, dvs. at kravet umiddelbart kan tvangsfuldbyrdes. Medmindre klagen er åbenbart grundløs, vil det dog oftest være hensigtsmæssigt at udskyde beslutningen om at videregive oplysningerne, indtil klagesagen er behandlet og afgørelsen meddelt skyldneren.

Det følger af lovforslagets *stk. 2*, at det er en betingelse, at den samlede gæld, jf. *stk. 1, nr. 2*, administreres af samme inddrivelsesmyndighed.

Det er endvidere en betingelse efter lovforslagets *stk. 3*, for videregivelse efter bestemmelsens *stk. 1, nr. 2*, at gælden kan inddrives ved udpantning, og der er fremsendt 2 rykkere til skyldneren, at der er foretaget eller forsøgt foretaget udlæg for kravet, at kravet er fastslået ved endelig dom, eller at det offentlige har erhvervet skyldnerens skriftlige erkendelse af den forfaldne gæld.

Med hensyn til den i *stk. 3* indeholdte betingelse vedrørende udpantningsret, er det fundet rimeligt at bestemme, at der udover den omstændighed, at gælden kan inddrives ved udpantning, tillige skal være fremsendt 2 rykkere til skyldneren. En lang række offentlige krav – herunder skatter og afgifter mv. – er tillagt udpantningsret.

Med hensyn til betingelsen om, at der skal være foretaget eller forsøgt foretaget udlæg, er det en forudsætning, at skyldneren har været til stede under udlægsforretningen. Det er således ikke tilstrækkeligt, at inddrivelsesmyndigheden har tilsagt skyldneren til en udlægsforretning, hvis skyld-

neren ikke er mødt op, eller hvis skyldneren ikke er truffet hjemme ved en udgående forretning.

Hvis kravet ikke er tillagt udpantningsret, vil videregivelse til private kreditoplysningsbureauer af oplysninger om gælden kun kunne ske, hvis kravet er fastslået ved dom eller hvis skyldneren, efter at kravet er forfaldent, skriftligt har erkendt den forfaldne gæld.

Der henvises til Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, side 63-65 og 277-282.

Til § 17

Af lovforslagets § 17 fremgår, at myndigheden skal give skyldneren skriftlig meddelelse herom, forinden videregivelse finder sted. Videregivelse må tidligst ske 4 uger efter, at denne meddelelse er givet.

Bestemmelsen bevirker for det første, at et sådant varsel vil give skyldneren mulighed for at rette henvendelse til myndigheden med henblik på at opklare eventuelle misforståelser, og for det andet vil varslet give skyldneren mulighed for at undgå videregivelsen ved at betale gælden, opnå henstand eller indgå en aftale om afdragsvis betaling af gælden.

Den skriftlige meddelelse, som først kan afgives, når betingelserne for videregivelse i forslagets § 16 er opfyldt, skal efter bestemmelsens *stk. 2* indeholde oplysning om, hvilke oplysninger der vil blive videregivet, til hvilket kreditoplysningsbureau oplysningerne vil blive videregivet, og hvornår videregivelse vil finde sted (normalt 4 uger efter). Meddelelsen skal endvidere indeholde oplysning om, at videregivelse ikke vil ske, hvis betaling af gælden sker inden videregivelsen, eller hvis der indrømmes henstand eller indgås og overholdes en aftale om afdragsvis betaling.

Når der er gået 4 uger fra meddelelsens afgivelse, kan videregivelse ske, medmindre gælden er betalt, eller der er bevilget henstand eller indgået en aftale om afdragsvis betaling. Hvis videregivelse undlades, fordi der på dette stadium indgås en aftale om afdragsvis betaling, skal der ikke – såfremt denne aftale ikke overholdes – ske meddelelse på ny efter forslagets § 17.

Hvis myndigheden efter udløbet af 4 ugers-fristen ikke i øvrigt uden ugrundet ophold videregiver de pågældende oplysninger til kreditoplysningsbureauet, og det ikke skyldes skyldnerens forhold, skal der gives

meddelelse på ny, såfremt myndigheden nu ønsker at foretage videregivelsen.

Det bemærkes, at en myndigheds beslutning om videregivelse af oplysninger om gæld til et kreditoplysningsbureau ikke er at betragte som en afgørelse i forvaltningslovens forstand.

Til § 18

Af lovforslagets § 18 fremgår, at vedkommende minister kan fastsætte nærmere regler om fremgangsmåden ved videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige.

Bestemmelsen svarer til persondatalovens § 18.

Det kan i den forbindelse bestemmes, at oplysninger om visse former for gæld til det offentlige ikke må videregives eller kun må videregives, hvis yderligere betingelser end de i § 16 nævnte er opfyldt.

Reglerne kan f.eks. gå ud på, at oplysninger om visse gældsforhold ikke må videregives. Fastsættelse af sådanne regler forudsættes navnlig at ske med hensyn til krav, der udspringer af bøder, der er pålagt virksomheder mv., idet allerede oplysninger om kreditormyndighedens identitet vil indebære en afsløring af, at de pågældende har begået et strafbart forhold. For så vidt angår privatpersoner bemærkes, at det allerede følger af forslaget § 15, stk. 2, at oplysninger om sådanne krav ikke må videregives.

Reglerne kan også gå ud på, at der skal iagttages visse yderligere eller skærpede betingelser end nævnt i den foreslåede § 16. Der kan eksempelvis fastsættes en højere beløbsgrænse for videregivelse af oplysninger om visse former for gæld.

Der henvises til Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, side 63-65 og 277-282.

Til kapitel 5

Kreditoplysningsbureauer

Til § 19

Lovforslagets § 19 fastslår, at den, som ønsker at drive virksomhed med behandling af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse (kreditoplysningsbureau), skal indhente tilladelse hertil fra Datatilsynet, inden behandlingen påbegyndes.

Bestemmelsen svarer til persondatalovens § 19. Den gældende praksis på området vil dermed fortsat være af betydning.

Reglerne om kreditoplysningsbureauers virksomhed tager sigte på al form for kreditoplysningsvirksomhed. Det er således uden betydning, hvem der måtte ønske at drive virksomhed med behandling af oplysninger til bedømmelse af soliditet og kreditværdighed med henblik på videregivelse. I praksis drives sådanne aktiviteter for tiden kun i den private sektor. De foreslåede regler tager derfor primært sigte herpå. Hvis offentlige myndigheder på et tidspunkt måtte ønske at påbegynde kreditoplysningsvirksomhed, følger det af reglen i § 19, at tilladelse hertil skal indhentes hos Datatilsynet.

Ordene ”driver virksomhed med” er indsat for at præcisere, at bestemmelsen ikke omfatter virksomheder eller andre, der i enkeltstående tilfælde eller lejlighedsvis skaffer sig, registrerer og videregiver soliditetsoplysninger til konkrete formål, f.eks. advokater. Derimod er det ikke herved sigtet til at begrænse bestemmelsen til kun at omfatte registreringsaktiviteter, der drives som traditionelle erhvervsvirksomheder, f.eks. som enkeltmandsfirmaer eller aktieselskaber. Eksempelvis vil også foreninger, der registrerer og videregiver soliditetsoplysning til medlemmerne, efter omstændighederne være omfattet af bestemmelsen. Derfor er bestemmelsen heller ikke formuleret således, at kun registreringsvirksomheder, der sælger oplysninger til udenforstående, er omfattet. Kriteriet er alene, at den pågældende indsamler og registrer soliditetsoplysninger med henblik på videregivelse.

Selv om virksomheden tillige og måske som hovedformål driver anden form for erhvervsvirksomhed, f.eks. inkassovirksomhed, bringer dette ikke virksomheden uden for kapitel 5, hvis betingelserne i § 19 er opfyldt.

Efter bestemmelsen skal den, der ønsker at drive denne form for virksomhed, forinden indgive anmeldelse herom til Datatilsynet. Efter forslaget § 36, stk. 1, skal Datatilsynet kunne fastsætte regler om, hvilken form og indhold en sådan anmeldelse skal have. Tilsynet vil på grundlag af anmeldelsen kunne vurdere, om virksomheden opfylder lovens krav.

Ordningen med indhentelse af tilladelse fra Datatilsynet til at drive virksomhed med kreditoplysningsbureau videreføres.

Et kreditoplysningsbureau skal derfor – inden virksomheden påbegyndes – foretage anmeldelse til Datatilsynet.

Der henvises til Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, side 108-118 og 277-282.

Til § 20

Efter bestemmelsen må kreditoplysningsbureauer kun registrere og videregive oplysninger, som efter deres art er af betydning for bedømmelse af økonomisk soliditet og kreditværdighed.

Bestemmelsen svarer til persondatalovens § 20 og indebærer dermed ikke ændringer i den gældende retstilstand. Den gældende praksis på området vil dermed fortsat være af betydning.

Det betyder bl.a., at et bureau ikke som led i kreditoplysningsvirksomheden kan indsamle oplysninger til belysning af f.eks. personen faglige evner mv. og dermed virke som en art ”ansættelsesnævn” for private virksomheder. Reglerne i § 20 forhindrer naturligvis ikke, at en virksomhed ved ansættelse af personale beder et kreditoplysningsbureau udtale sig om en ansøgers økonomiske soliditet eller kreditværdighed. Denne behandling vil dog under alle omstændigheder skulle leve op til kravene i forordningens artikel 5.

Det betyder endvidere bl.a., at et kreditoplysningsbureau ikke må registrere oplysninger om fordringer, der er bestridt af skyldneren, såfremt fordringen ikke har været forelagt en retslig instans. Baggrunden herfor er, at der i så fald ikke er tale om registrering af oplysninger om betalingsevne, men derimod registrering af oplysninger om betalingsvilje.

Når et bureau registrerer oplysninger til brug for bedømmelse af en persons eller virksomheds økonomiske soliditet og kreditværdighed, må oplysningerne kun vedrøre netop denne person eller virksomhed.

I *stk. 2* fastsættes et forbud mod, at følsomme oplysninger og oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger behandles af kreditoplysningsbureauer.

Der er således indført et absolut forbud mod at registrere eller videregive oplysninger som nævnt i forordningens artikel 9, stk. 1, om bl.a. race, religion og om helbredsforhold samt oplysninger om strafbare forhold som nævnt i forordningens artikel 10. Der er i det væsentlige tale om oplysninger, som allerede efter stk. 1 ikke må registreres og videregives. At man desuagtet har fastsat forbuddet i stk. 2 og herved fjernet enhver fortolkningstvivl omkring disse præcist angivne oplysninger, skyldes, at der er tale om oplysninger af følsom karakter, hvis registrering ikke blot vil være i strid med hensynet til det enkelte menneskets frihed, men også med et ønske om at beskytte minoritetsgrupper.

Bestemmelsen i stk. 2 bevirker dog ikke, at kreditoplysningsbureauer ikke kan behandle oplysninger som nævnt i forordningens artikel 9, stk. 1 eller 10, såfremt der er tale om begæringer fra den registrerede efter reglerne i forordningens kapitel III.

I *stk. 3* bestemmes, at oplysninger om forhold, der taler imod kreditværdighed, og som er mere end 5 år gamle, ikke må registreres eller videregives, medmindre det i det enkelte tilfælde er åbenbart, at forholdet er af afgørende betydning for bedømmelsen af den pågældendes økonomiske soliditet og kreditværdighed. Objektive oplysninger, som f.eks. identifikationsoplysninger, bør ifølge sagens natur ikke være genstand for forældelse og er ikke omfattet af bestemmelsen. Der ses heller ikke at være behov for en forældelsesregel vedrørende oplysninger, der er ”positive” for den pågældende. Adgangen til i meget begrænset omfang at registrere eller videregive oplysninger om forhold, der er mere end 5 år gamle er medtaget, fordi navnlig visse former for betalingsstandsning, som f.eks. konkurs, efter omstændighederne fortsat kan være så relevante for den økonomiske bedømmelse, at der bør være adgang til at videregive oplysningen om forholdet ud over 5-årsfristen.

Kreditoplysningsbureauet må endvidere ikke benytte en oplysning, der er forældet efter denne bestemmelse, som grundlag for en bedømmelse, selv om selve oplysningen ikke herved videregives.

I *stk. 4* bestemmes, at databeskyttelsesforordningens artikel 12-19 gælder for behandling af oplysninger om virksomheder mv., hvis denne behandling udføres for kreditoplysningsbureauer.

Bestemmelsen indebærer, at også registrerede virksomheder mv. – som et kreditoplysningsbureau behandler oplysninger, der ikke er personoplysninger, om – har samme ret (som ved registrering af personoplysninger) til at gøre indsigelse og få berigtiget samt slettet oplysninger mv. Endvidere har kreditoplysningsbureauer også oplysningspligt i forbindelse med oplysninger, der ikke er personoplysninger.

Der henvises til Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, side 108-118 og 277-282.

Til § 21

I denne bestemmelse fastsættes nærmere regler om, *hvorledes* kreditoplysningsbureauer må videregive oplysninger.

Bestemmelsen i *stk. 1* svarer – med en enkelt ændring – til persondatalovens § 23, stk. 1. Den gældende praksis på området vil dermed fortsat være af betydning.

Som en konsekvens af databeskyttelsesforordningen finder stk. 1 – modsat stk. 1 i persondataloven – ikke anvendelse på den registrerede, idet den registreredes rettigheder fremover alene reguleres af bestemmelserne i databeskyttelsesforordningen og lovforslagets generelle bestemmelse herom.

Efter forslaget skal oplysningerne som hovedregel meddeles abonnenter skriftligt. Herved sikres fornødent bevis for, hvad der er oplyst til tredje-mand, hvilket er et nødvendigt led i den kontrol mv., der etableres efter reglerne i kapitel 5.

Et ufravigeligt krav om skriftlighed er for så vidt at foretrække, men det kan dels være meget bekosteligt for bureauerne, og en hindring for at efterkomme erhvervslivets behov for hurtigt at kunne få oplysningerne.

Der er som regel tale om meddelelse af kortfattede enkeltoplysninger, f.eks. om, hvorvidt en registreret er under konkurs, har næringsbrev eller ejer fast ejendom. Derfor er der efter bestemmelsen i stk. 1, 2. pkt., mulig-

hed for, at kortfattede oplysninger kan meddeles mundtligt til abonnenter, såfremt spørgerens navn og adresse noteres og opbevares i mindst 6 måneder. Notering af navn og adresse på spørgeren er nødvendig af hensyn til forordningens artikel 19, hvorefter 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.

Halvårsfristen er begrundet i, at forespørgere normalt kun vil benytte nyligt indhentede oplysninger som grundlag for kreditværdighedsvurderinger, hvorfor der i en berigtigelsessituation ikke vil være samme hensyn til at foretage berigtigelse i relation til meget gamle besvarelser. Endvidere vil spørgsmålet om, hvorvidt en oplysning er korrekt eller ej, normalt blive aktuelt ret kort efter videregivelsen, hvis der overhovedet er anledning til at rejse det. Efter forordningens artikel 19 skal der dog – uanset 6 måneders fristen for opbevaring af spørgerens navn og adresse – ske berigtigelse, medmindre dette viser sig umuligt eller er uforholdsmæssigt vanskeligt.

Efter *stk. 2* må kreditoplysningsbureauer kun udsende publikationer, såfremt det sker til abonnenter, og publikationerne kun indeholder oplysninger i summarisk form.

Bestemmelsen i *stk. 2* svarer til persondatalovens § 23, *stk. 2*. Den gældende praksis på området vil dermed fortsat være af betydning.

Bestemmelsen indeholder herved et forbud mod offentliggørelse af publikationer indeholdende oplysninger i summarisk form.

Sådanne publikationer kan være publikationer, der i kort skematisk form giver oplysninger om næringsdrivende til abonnenter. Med ordene ”i summarisk form” sigtes til kortfattede fælles-oplysninger af bestemte typer, der som regel er opstillet i skemaform og tit besvaret med ”ja” eller ”nej”.

Foruden navn og adresse kan der være tale om oplysninger om f.eks. etableringsår, omsætningens størrelse, kreditværdighedsklasse, om vedkommende er under konkurs, eller om vedkommende ejer fast ejendom og lignende oplysninger.

Efter justitsministeriets opfattelse bør det fortsat være muligt for kreditoplysningsbureauerne at udsende publikationer med oplysninger i summarisk

indhold til faste abonnenter. For de registrerede er det for så vidt en betryggelse, at der er tale om et ret »åbent register«, men oplysningerne er dog ofte af så privat karakter, at en egentlig offentliggørelse ville kunne føles som en krænkelse af den private fred. Derfor bestemmes i stk. 2, at sådanne publikationer kun må udsendes til abonnenter, og offentligt salg må således ikke finde sted. Offentligt salg vil ikke blot foreligge ved salg f.eks. via boghandlere ved salg i butikker eller online, men også ved salg til enhver direkte fra bureauet.

Publikationerne må efter stk. 2, 2. pkt., ikke indeholde oplysninger om de registreredes personnumre. Baggrunden for bestemmelsen er, at der ikke på denne måde bør gives en generel adgang til videregivelse af større samlinger af personnumre.

Bestemmelsen i *stk. 3* svarer til persondatalovens § 23, stk. 3, hvorefter summariske oplysninger om skyldforhold kun må videregives, hvis en række nærmere oplistede betingelser er opfyldt.

Kreditoplysningsbureauets videregivelse af oplysninger om kreditværdighed til bureauets abonnenter sker dels i form af såkaldt bredere bedømmelser, dels som summariske kreditoplysninger.

Registrerede oplysninger om kreditværdighed må kun videregives i summarisk form, hvis oplysningerne hidrører fra Statstidende, eller hvis oplysningerne vedrører skyldforhold til samme kreditor på mere end 1.000 kr. Ved de sidstnævnte skyldforhold er det desuden en betingelse for videregivelse, at kreditor har erhvervet den registreredes skriftlige erkendelse af en forfalden gæld, eller at der er foretaget retslige skridt mod den pågældende.

Som følge af betingelserne for videregivelse af summariske kreditoplysninger er abonnenterne forpligtede til at dokumentere, at fordringen er større end 1.000 kr., samt at debitor har erkendt den forfaldne gæld enten i form af en underskrevet skylderklæring eller et frivilligt forlig eller, at kreditor har foretaget retslige skridt mod debitor, f.eks. udtaget stævning.

Det følger endvidere af bestemmelsen i stk. 3, 2. pkt., at oplysninger om endeligt godkendt gældssanering dog ikke må videregives.

Bestemmelsen i stk. 3, 3. pkt., præciserer, at betingelserne for videregivelse af summariske oplysninger også skal være opfyldt, hvis sådanne oplys-

ninger videregives i forbindelse med udarbejdelse af bredere kreditbedømmelser.

Bestemmelsen i *stk. 4* svarer til persondatalovens § 23, stk. 4, hvorefter videregivelse af summariske oplysninger om enkeltpersoners skyldforhold kun må ske på en sådan måde, at oplysningerne ikke kan danne grundlag for vurderingen af økonomisk soliditet.

Det forudsættes, at bestemmelsen i *stk. 4* ikke er til hinder for, at kreditoplysningsbureauerne videregiver oplysninger opdelt efter postnumre. Der henvises herved til Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, side 281 f.

Der henvises til Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, side 108-118 og 277-282.

Til § 22

Reglerne om de registreredes rettigheder, som fremgår af databeskyttelsesforordningens kapitel III finder anvendelse på behandling efter lovforslaget. For nærmere om gennemsigtig oplysning og processuelle spørgsmål om registreredes rettigheder, jf. forordningens artikel 12, se *betænkningen* side 262-279, oplysningspligt ved indsamling hos den registrerede, jf. forordningens artikel 13, se *betænkningen* side 279-296, om oplysningspligt, hvis personoplysningerne ikke er indsamlet hos den registrerede, jf. forordningens artikel 14, se *betænkningen* side 296-312 samt om indsigtsretten, jf. forordningens artikel 15, se *betænkningen* side 315-325, 373-374 samt 387-389.

Lovforslagets § 22, stk. 1 og 2, svarer stort set til persondatalovens §§ 30, 32, stk. 1, og 39, stk. 3.

I lovforslagets § 22, *stk. 1 og 2*, er fastsat regler om, i hvilket omfang den dataansvarlige kan gøre undtagelse fra den oplysningspligt og indsigtsret, som følger af databeskyttelsesforordningens artikel 13, stk. 1-3, artikel 14, stk. 1-4 og artikel 15.

Henvisningen til artikel 12 i databeskyttelsesforordningen er medtaget, idet bestemmelsen indeholder en række generelle betingelser for, hvordan og hvornår den dataansvarlige skal kommunikere, når der sker opfyldelse

af oplysningspligten efter artikel 13 og 14 og indsigtsretten efter artikel 15.

Lovforslagets stk. 1 og 2 har for så vidt angår artikel 13, stk. 1-3, og 14, stk. 1-4, kun betydning, hvis underretning af den registrerede ikke kan undlades efter undtagelsesbestemmelserne i artikel 13, stk. 4, artikel 14, stk. 5, og for så vidt artikel 15, stk. 4.

I den forbindelse henvises specifikt til det anførte i *betænkningen* side 294, 307-311 og 323-324. Opmærksomheden henledes i den forbindelse på det anførte på side 310, hvorefter forordningens artikel 14, stk. 5, litra d, ses at indebære en undtagelsesmulighed, der svarer til den gældende persondatalovs § 32, stk. 2, (se lovforslagets § 22, stk. 3) om indsigtsretten med henvisningen heri til offentlighedslovens § 35, der indebærer, at der ikke er indsigt i sager omfattet af særlige bestemmelser om tavshedspligt, såsom skatteforvaltningslovens § 17. Samme undtagelse ses således med henvisningen til ”lovbestemte tavshedspligt” i forordningens artikel 14, stk. 5, litra d, at være indført vedrørende oplysningspligten efter artikel 14 – en undtagelse, der ikke er gældende i dag, da persondatalovens § 29, stk. 2-3, og § 30 om undtagelser fra oplysningspligten ikke indeholder en undtagelsesmulighed svarende til persondatalovens § 32, stk. 2.

Indskrænkningen i den dataansvarliges eller dennes repræsentants oplysningspligt efter lovforslagets § 22, stk. 1-2, kan kun ske på baggrund af en konkret afvejning af de modstående interesser, som er nævnt i bestemmelserne. Afvejningen må foretages for hver enkelt oplysning for sig med den virkning, at der, såfremt sådanne hensyn kun gør sig gældende for en del af de i artikel 13, stk. 1-3 og artikel 14, stk. 1-4, nævnte oplysninger, skal der gives den registrerede meddelelse om de øvrige oplysninger.

Afvejningen af de modstående interesser i forbindelse med begrænsningen af indsigtsretten må tillige foretages for hver enkelt oplysning for sig med den virkning, at den registrerede, såfremt afgørende hensyn til private eller offentlige interesser kun gør sig gældende for en del af de oplysninger, som behandles hos den dataansvarlige, skal gøres bekendt med de øvrige oplysninger. Der er ikke efter bestemmelsen adgang til generelt at undtage bestemte former for behandling af oplysninger fra indsigtsretten.

Efter bestemmelsen i *stk. 1* kan undtagelse fra bestemmelserne i artikel 13, stk. 1-3, artikel 14, stk. 1-4, og artikel 15, gøres, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til *private interesser*, herunder hensynet til den pågældende selv.

I afvejningen indgår som nævnt på den ene side den registreredes interesse i at få kendskab til de i artikel 13, stk. 1-3, og artikel 14, stk. 1-4, nævnte oplysninger. Heroverfor står på den anden side hensynet til private interesser, herunder til den pågældende selv. De private interesser, som kan beskyttes efter bestemmelsen, er såvel den dataansvarliges som tredjemands interesser.

Som private interesser, der bl.a. vil kunne begrunde hemmeligholdelse, kan nævnes forretningshemmeligheder, den professionelle tavshedspligt, som læger og advokater skal iagttage, retten til at forberede sit eget forsvar i retssager samt beskyttelse af menneskerettighederne.

Endvidere vil bl.a. afgørende hensyn til en dataansvarlig, der indsamler oplysninger om den registrerede, kunne begrunde hemmeligholdelse, eksempelvis hvis formålet med indsamlingen forspildes, hvis den registrerede får kendskab til indsamlingen.

I stk. 1 fastsættes det endvidere, i hvilket omfang den dataansvarlige kan undlade at give den registrerede ret til indsigt efter forordningens artikel 15. Af bestemmelsen følger, at den registrerede ikke har krav på indsigt, hvis vedkommendes interesse i at få kendskab til oplysninger findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv.

Efter en konkret vurdering vil det være muligt at nægte indsigt i oplysninger, hvis dette vil medføre, at virksomhedens forretningsgrundlag, forretningspraksis eller know-how derved vil lide væsentlig skade. Det vil endvidere efter en konkret vurdering være muligt at nægte indsigt i interne vurderinger af, hvorvidt virksomheden på basis af foreliggende oplysninger vil indgå et kontraktforhold, ændre et bestående kontraktforhold, stille særlige vilkår for fortsættelse, eventuelt helt opsige et kontraktforhold og lignende tilfælde. På samme måde vil det efter omstændighederne være muligt at nægte indsigt i f.eks. et notat, der vurderer, hvorvidt der er udsigt til, at en bestemt retssag mod en kunde kan vindes, eller et internt notat i en sag, der påpeger mulige tegn på, at en kunde har forsøgt at udøve forsikringssvig over for et forsikringsselskab eller forsøgt at unddrage sig forpligtelsen i medfør af f.eks. en lånekontrakt.

Vedrørende den indsigtsret, der følger af forordningens artikel 15, stk. 1, litra h, om information om forekomsten af automatiske afgørelser, herun-

der profilering, som omhandlet i artikel 22, stk. 1 og 4, vil den dataansvarlige eksempelvis ikke være forpligtet til at udlevere oplysninger, som må anses for at være forretningshemmeligheder, eller som er beskyttet efter den immaterielle lovgivning, herunder ophavsretsloven.

Med anvendelsen af udtrykket »afgørende« i bestemmelsen er det tilkendegivet, at undtagelse fra oplysningspligten og indsigtsretten kun kan gøres, hvor der er nærliggende fare for, at privates interesser vil lide skade af væsentlig betydning.

Efter bestemmelsen i *stk. 2* kan undtagelse fra bestemmelserne i artikel 12, 13, stk. 1-3, artikel 14, stk. 1-4, og artikel 15 tillige gøres, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til *offentlige interesser*, herunder navnlig hensynet til statens sikkerhed, forsvaret, den offentlige sikkerhed, forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed, 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, beskyttelse af retsvæsenets uafhængighed og retssager, forebyggelse, efterforskning, afsløring og retsforfølgning i forbindelse med brud på etiske regler for lovregulerede erhverv, kontrol-, tilsyns- eller reguleringsfunktioner, herunder opgaver af midlertidig karakter, der er forbundet med offentlig myndighedsudøvelse i nogle af de tilfælde, der er omhandlet ovenfor, beskyttelse af den registrerede eller andres rettigheder og frihedsrettigheder, og håndhævelse af civilretlige krav.

Bestemmelsen fastsætter – ligesom bestemmelsen i stk. 1 – at indskrænkning i den dataansvarliges eller dennes repræsentants oplysningspligt kun kan ske på grundlag af en konkret afvejning af de modstående interesser, som er nævnt i bestemmelsen. På baggrund af en sådan afvejning vil undtagelse kunne gøres, hvis der er nærliggende fare for, at det offentliges interesser vil lide skade af væsentlig betydning.

I bestemmelsen fastsættes det endvidere, i hvilket omfang den dataansvarlige kan undlade at give den registrerede ret til indsigt. Indskrænkningen i den registreredes adgang til at blive gjort bekendt med de i forordningens artikel 15, nævnte oplysninger, kan efter bestemmelsen kun ske på grund-

lag af en konkret afvejning af de modstående interesser. Der kan endvidere også ske undtagelse fra indsigtsretten efter artikel 15, stk. 1, litra h, som omhandler indsigte i forbindelse med automatiske afgørelser, herunder profilering, som omhandlet i forordningens artikel 22, stk. 1 og 4.

I afvejningen om særligt undtagelse fra indsigtsretten efter forordningens artikel 15 indgår som nævnt på den ene side den registreredes interesse i at få kendskab til oplysningerne. Hermed sigtes ikke blot til den registreredes interesse i kendskab til oplysningerne i forbindelse med overvejelser om indbringelse af en sag, hvori de indsamlede oplysninger indgår, for domstolene, højere administrativ myndighed, vedkommende tilsynsmyndighed eller Folketingets Ombudsmand, men også til den registreredes interesse i at kunne kontrollere oplysningernes rigtighed med henblik på den dataansvarliges anvendelse af oplysningerne.

Med anvendelsen af udtrykket »afgørende« i bestemmelsen er det tilkendegivet, at undtagelse fra oplysningspligten og indsigtsretten kun kan gøres, hvor der er nærliggende fare for, at offentlige interesser vil lide skade af væsentlig betydning.

Med udtrykket »afgørende hensyn« tilsigtes kongruens og overensstemmelse med den tilsvarende afvejning af modsatrettede hensyn, som skal foretages efter offentlighedslovens § 8 om egenaccess og forvaltningslovens § 15, § 15 a og § 15 b om undtagelse af oplysninger fra aktindsigt.

I overensstemmelse med forordningens artikel 23, stk. 2, skal den dataansvarlige i videst muligt og relevant omfang – når der konkret gøres undtagelse fra oplysningspligten og indsigtsretten efter *både stk. 1 og 2* – forsøge at tage højde for de hensyn, som følger af artikel 23, stk. 2, inden for det livsområde, som den dataansvarlige vil begrænse.

Dette betyder eksempelvis, at den dataansvarlige er forpligtet til at overveje, hvilke risici, der er forbundet med undtagelse fra oplysningspligten eller indsigtsretten for den registrerede, jf. artikel 23, stk. 2, litra g. Således f.eks. om der vil være en risiko for, at de indsamlede oplysninger er forkerte.

Endvidere vil den dataansvarlige eksempelvis i forbindelse med undtagelse fra indsigtsretten af hensyn til andres frihedsrettigheder kunne underrette den registrerede om denne begrænsning, jf. artikel 23, stk. 2, litra h.

Endelig påhviler det direkte efter bestemmelsen i stk. 1 og 2 den dataansvarlige at tage hensyn til rækkevidden af de indførte begrænsninger, jf. artikel 23, stk. 2, litra c, idet den dataansvarlige skal foretage en konkret vurdering af, om der er afgørende hensyn, for hver enkelt oplysning for sig.

I bestemmelsens *stk. 3* fastsætte det, at oplysninger, der behandles for den offentlige forvaltning som led i administrativ sagsbehandling, kan undtages fra retten til indsigt efter databeskyttelsesforordningens artikel 15, stk. 1, i samme omfang som efter reglerne i §§ 19-29 og 35 i lov om offentlighed i forvaltningen.

Bestemmelses svarer til persondatalovens § 32, stk. 2.

Bestemmelsen er indsat for at sikre, at forvaltningsmyndigheders behandling af oplysninger kan undtages fra den registreredes ret til indsigt i samme udstrækning som efter offentlighedslovens regler om egenacces, jf. offentlighedslovens § 8.

Det forudsættes, at bestemmelsen også kan anvendes på myndigheder, som ikke er undergivet offentlighedsloven, når disse myndigheder udfører administrativ sagsbehandling.

Det forudsættes endvidere, at bestemmelsen også kan anvendes på Procesbevillingsnævnet, uanset at dette er et uafhængigt nævn, der virker i nær tilknytning til domstolssystemet.

Af lovforslagets *stk. 4, 1. pkt.*, følger, at der ikke er ret til indsigt i oplysninger, der behandles for domstolene, hvis oplysningerne indgår i tekst, som ikke foreligger i endelig form. Dette gælder dog ikke, hvis oplysningerne er videregivet til en tredjemand, jf. *2. pkt.*

Bestemmelses svarer til persondatalovens § 32, stk. 3.

Udtrykket oplysningerne indgår i tekst, som ikke foreligger i endelig form tager sigte på den situation, at de oplysninger, som der begæres indsigt i, er under bearbejdning i form af, at oplysningerne indgår i et udkast mv. Dette vil bl.a. kunne være et udkast til dom eller kendelse. Også udkast til retsbog og lignende vil være omfattet af udtrykket. Det bemærkes i den forbindelse, at domme først vil foreligge i endelig form, når de er afsagt i et offentligt retsmøde. Også oplysninger i tekst, der er under udarbejdelse i

forbindelse med domstolenes udøvelse af administrativ virksomhed, vil kunne undtages fra indsigtsretten.

Dette gælder dog som nævnt ikke, hvis oplysningerne er videregivet til en tredjemand. For så vidt angår betydningen af begrebet tredjemand henvises til databeskyttelsesforordningens artikel 4, nr. 10. Det bemærkes, at der selvsagt ikke efter lovforslagets § 22, stk. 4, vil være tale om videregivelse til tredjemand, når flere dommere deltager i en sags behandling og i den forbindelse forelægger hinanden udkast til domme mv.

Af bestemmelsens 3. pkt. følger, at registrerede personer ikke har ret til indsigt i oplysninger i voteringsprotokoller og andre referater af domstolenes rådslagning samt materiale udarbejdet af domstolene til brug for rådslagningen. Med bestemmelsen sikres det, at der – ligesom efter den nuværende retstilstand – ikke er ret til indsigt i domstolenes voteringsprotokoller og andet materiale, der afspejler rådslagningen i domstolenes civile sager. Efter bestemmelsen vil der heller ikke være ret til indsigt i det materiale, som udarbejdes alene med det formål at danne grundlag for selve rådslagningen, f.eks. de referater i skriftligt behandlede civile sager i Højesteret, som udarbejdes af en dommerfuldmægtig, og som danner grundlag for voteringen.

Udtrykket »materiale udarbejdet af domstolene til brug for rådslagningen« omfatter derimod f.eks. ikke processkrifter i civile sager, idet disse ikke udarbejdes af domstolene. Uden for udtrykket falder endvidere retsbøger med vidneforklaringer mv. Dette skyldes, at sådant materiale, der udarbejdes af domstolene, og som for så vidt anvendes i forbindelse med rådslagningen, ikke udarbejdes alene med henblik herpå.

De begrænsninger i retten til indsigt, som følger af den foreslåede bestemmelse, gælder, uanset om der – efter de herom gældende retningslinjer – gives tilladelse til tredjemand til at foretage gennemsyn af voteringsprotokoller mv. til brug for det praktiske retsliv eller faglitterær virksomhed.

Det bemærkes, at lovforslagets regler om den registreredes indsigtsret ikke finder anvendelse på behandling af personoplysninger, som foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed, forordningens artikel 2, stk. 2, litra d.

Bestemmelsens *stk. 5* fastsætter, at visse særlige typer af behandling af oplysninger ikke er undergivet den registreredes indsigtsret.

Efter bestemmelsen er der ikke ret til indsigt i oplysninger, der udelukkende behandles med videnskabelig forskning for øje.

Bestemmelsen svarer til persondatalovens § 32, stk. 4.

Også behandling af personoplysninger i statistisk øjemed er efter bestemmelsen undtaget fra retten til indsigt. En betingelse herfor er dog, at oplysningerne kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker. Bestemmelsen viderefører den gældende retstilstand.

Der henvises i øvrigt til afsnit 2.4. i lovforslagets almindelige bemærkninger.

Til § 23

Det følger af forordningens artikel 13, stk. 3, og artikel 14, stk. 4, at der gælder en fornyet oplysningspligt for den dataansvarlige over for den registrerede, hvis den dataansvarlige agter at viderebehandle personoplysningerne til et andet formål end det, hvortil de er indsamlet.

Med bestemmelsen foreslås det, at oplysningspligten efter artikel 13, stk. 3, og artikel 14, stk. 4, ikke finder anvendelse, når offentlige myndigheder viderebehandler personoplysninger til et andet formål end det, hvortil de er indsamlet, og viderebehandlingen sker på baggrund af regler fastsat efter den foreslåede § 5, stk. 3.

Det foreslås således, at den fornyede oplysningspligt generelt ikke skal gælde for offentlige myndigheders viderebehandling af personoplysninger til andre formål, end de er indsamlet til, i tilfælde hvor vedkommende minister har udnyttet bemyndigelsen i lovforslagets § 5, stk. 3, og i bekendtgørelsesform bestemt, at en nærmere angiven viderebehandling af personoplysninger lovligt skal kunne finde sted i den offentlige forvaltning.

Der henvises i øvrigt til afsnit 2.4.3.5. i lovforslagets almindelige bemærkninger.

Til § 24

I denne bestemmelse fastsættes nærmere regler om databeskyttelsesrådgiveres tavshedspligt. Efter bestemmelsen må databeskyttelsesrådgivere således ikke uberettiget videregive eller udnytte oplysninger, som de under udøvelsen af deres hverv som databeskyttelsesrådgivere er blevet bekendt med.

Den strafbare handling beror på, om der er tale om en ”uberettiget” videregivelse eller udnyttelse af oplysninger, som databeskyttelsesrådgivere under udøvelsen af deres hverv som databeskyttelsesrådgivere er blevet bekendt med. Udtrykket ”uberettiget” angiver, at der skal være tale om en retsstridig videregivelse eller udnyttelse af oplysninger, hvorefter videregivelsen er i strid med lovforslagets § 24.

Det betyder, at oplysninger om f.eks. en organisations påtænkte omstrukturering, strategiske overvejelser eller lignende, som databeskyttelsesrådgivere under udøvelsen af deres hverv er blevet bekendt med – efter omstændighederne – kan anses for omfattet af databeskyttelsesrådgiveres tavshedspligt efter lovforslagets § 24.

For så vidt angår betydningen af offentligt ansatte databeskyttelsesrådgiveres tavshedspligt, henvises i øvrigt til forvaltningslovens § 27 og straffelovens § 152 og §§ 152 c-152 f.

Det er forbundet med bødestraf, hvis databeskyttelsesrådgivere ”uberettiget” videregiver eller udnytter oplysninger, som de under udøvelsen af deres hverv som databeskyttelsesrådgivere er blevet bekendt med, jf. lovforslagets § 41, stk. 7.

Der henvises i øvrigt til lovforslagets § 41, stk. 7, og bemærkningerne her-til.

Til § 25

Lovforslagets § 25 fastslår, at det er Datatilsynet, der er bemyndiget til at akkreditere certificeringsorganer, jf. databeskyttelsesforordningens § 43, stk. 1, litra a. Der henvises i øvrigt til lovforslagets almindelige bemærkninger, afsnit 2.5.3.2.

Til § 26

Bestemmelsen i *stk. 1* foreskriver et krav om, at der skal indhentes en tilladelse fra Datatilsynet inden iværksættelsen af visse typer af behandlinger.

Bestemmelsen svarer – for så vidt angår advarselsregistervirksomhed og kreditoplysningsbureauvirksomhed samt behandling, som udelukkende finder sted med henblik på at føre retsinformationssystemer – til reglerne i persondatalovens § 50, stk. 1, nr. 2, 3 og 5.

Der skal efter bestemmelsen ske forelæggelse for Datatilsynet, før iværksættelse af sådan virksomhed.

Det overlades til Datatilsynet i hvert enkelt tilfælde at afgøre, om oprettelsen af sådanne registre tjener anerkendelsesværdige interesser, og i bekræftende fald at give individuelle forskrifter med hensyn til registrerets brug.

I Datatilsynets bedømmelse af, om en ansøgning bør imødekommes, må navnlig indgå en vurdering af registrets formål i forhold til den risiko for krænkelse af privatlivets fred, som oprettelse og brugen af registret kan medføre. Der kan eksempelvis fastsættes særlige sikkerhedsforanstaltninger og stilles sådanne andre vilkår, som i hvert enkelt tilfælde skønnes nødvendige. Det vil f.eks. kunne være, at registret skal slettes efter en vis tid, eller at bestemte oplysninger skal slettes efter en vis periode.

Det afgørende for, om et register er omfattet af bestemmelsen i stk. 1, nr. 1, om et *advarselsregister*, er, at registret er oprettet med henblik på videregivelse. At der jævnligt sker videregivelse af oplysninger fra et register, der primært er oprettet med et andet formål, medfører ikke, at registret bliver omfattet af bestemmelsen. Omfattet af bestemmelsen vil derimod f.eks. typisk være et register, der er oprettet af en forening eller en brancheorganisation med henblik på at videregive oplysninger til foreningens eller brancheorganisationens medlemmer om medlemmernes forretningsforbindelse og disses betalingsevne. Sådanne advarselsregistre kan eksempelvis være Teleindustriens advarselsregister over personer og/eller virksomheder, som kun kan tegne abonnement efter en særlig vurdering, eller et advarselsregister over lejere, der har misligholdt deres lejemål eller lejeaftale.

For de behandlinger der udelukkende finder sted med henblik på at føre retsinformationssystemer sigtes til retsinformationssystemer, der er omfattet af lovforslagets § 9.

For nærmere om kreditoplysningsområdet se afsnit 2.3.11. og de specielle bemærkninger til kapitel 4 og 5.

I *stk. 2* er indsat en bemyndigelsesbestemmelse, hvorefter justitsministeren kan undtage behandlinger, der er omfattet af *stk. 1* fra tilladelseskravet.

Bestemmelsen i *stk. 2* svarer til persondatalovens § 50, *stk. 3*.

I henhold til *stk. 3* kan justitsministeren fastsætte regler om, at der forinden iværksættelsen af andre behandlinger end de i *stk. 1* nævnte skal indhentes en tilladelse fra Datatilsynet. Der kan der f.eks. lægges vægt på, om der er tale om en behandling, som har til formål at udelukke den registrerede fra at udøve en ret, modtage en ydelse eller opnå en kontrakt, eller som indebærer anvendelse af ny teknologi, der indebærer særlige risici for registrerede personer.

Bestemmelsen i *stk. 3* svarer til persondatalovens § 50, *stk. 4*.

Når bemyndigelsen til at fastsætte regler om indhentning af tilladelse fra Datatilsynet i *stk. 3* udnyttes, er det efter forordningens artikel 36, *stk. 5*, tillige et krav, at der skal være tale om en behandling under udførelsen af en *opgave i samfundets interesse*.

Af bestemmelsens *stk. 4* følger, at Datatilsynet kan fastsætte nærmere vilkår for udførelsen af behandlinger, som skal tillades efter *stk. 1* eller *3*. Ved fastsættelsen af vilkår for behandlinger af oplysninger forudsættes det, at der tages udgangspunkt i de vilkår, som i dag stilles i henhold til persondataloven. Herudover kan vilkårene for de nævnte erhvervsmæssige aktiviteter udformes som en nærmere beskrivelse af lovens krav samt indskærpelse af kravene til sikkerhedsforanstaltninger.

Bestemmelsen svarer til persondatalovens § 50, *stk. 5*.

Af bestemmelsens *stk. 5* følger det, at Datatilsynets tilladelse skal indhentes på ny, hvis der er tale om væsentlige ændringer i de i *stk. 1* eller *3* nævnte behandlinger. Tilsynets tilladelse til ændringen skal indhentes in-

den iværksættelsen, idet der dog ikke skal indhentes tilladelse, såfremt der er tale om ændringer af mindre væsentlig betydning.

Når lovforslaget træder i kraft, vil det ikke være nødvendigt at indhente en ny tilladelse til en fortsat behandling, som Datatilsynet har givet tilladelse til efter persondatalovens § 50, stk. 1, nr. 2-3, men Datatilsynets tilladelse skal dog også fremover indhentes på ny, hvis der er tale om væsentlige ændringer.

Bestemmelsen svarer delvist til persondatalovens § 51, stk. 2.

Der henvises i øvrigt til afsnit 2.6.3. i lovforslagets almindelige bemærkninger.

Til kapitel 10

Datatilsynet

Til § 27

Det foreslås i lovforslagets *stk. 1*, at Datatilsynet, der består af et råd og et sekretariat, skal føre tilsyn med enhver behandling, der omfattes af loven, jf. dog kapitel 11 om tilsyn med domstolene.

Denne ordning svarer i vidt omfang til den gældende ordning i persondataloven.

Med den foreslåede bestemmelse får tilsynet til opgave at føre tilsyn med behandling, der er omfattet af loven, databeskyttelsesforordningen og anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger.

Der henvises i øvrigt til afsnit 2.7.3.1. i lovforslagets almindelige bemærkninger.

Det foreslås i lovforslagets *stk. 2*, at tilsynets daglige forretninger varetages af et sekretariat, der ledes af en direktør.

Der sker således med den foreslåede bestemmelse en videreførelse af den gældende ordning.

Det fremgår af persondatalovens § 55, stk. 3, at, Datarådet, der 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.

Det fremgår af forarbejderne til persondataloven (Folketingstidende 1999-2000, tillæg A, side 4101), at der ved udpegning af medlemmer af rådet skal tilstræbes uvildighed og sagkundskab.

Det foreslås i lovforslagets *stk. 3*, at justitsministeren nedsætter Datarådet, som består af en formand, der er dommer, og af 7 andre medlemmer. Erhvervsministeren og ministeren for offentlig innovation udnævner hver ét af de 7 andre medlemmer. Justitsministeren udnævner således formanden og 5 af medlemmerne, ligesom justitsministeren kan udpege stedfortrædere for medlemmerne. Formanden, medlemmerne og stedfortræderne for disse udpeges for 4 år. Der kan ske genudpegning to gange. Udpegelsen af formand, medlemmer og stedfortrædere for disse sker på baggrund af disses faglige kvalifikationer, og der skal ved udpegningen tilstræbes uvildighed og saglighed. Endvidere bør det tilstræbes, at der udpeges et eller flere medlemmer med erfaring inden for informationssikkerhed og anvendelse af data i praksis.

Der sker med den foreslåede bestemmelse en videreførelse af reglerne om Datarådets nedsættelse med den ændring, at der alene kan ske genudpegning to gange.

Det fremgår af persondatalovens § 55, stk. 4, at Datarådet fastsætter sin forretningsorden og de nærmere regler om arbejdets fordeling mellem råd og sekretariat.

Det foreslås i lovforslagets *stk. 4*, at bemyndigelsen til, at Datarådet kan fastsætte sin forretningsorden og fordelingen af arbejdet mellem rådet og sekretariatet videreføres.

Det foreslås i lovforslagets *stk. 5* at udpegelsen af formand, medlemmer og stedfortrædere for disse er betinget af, at de pågældende sikkerhedsgodkendes, og at godkendelsen opretholdes i hele embedsperioden.

Der skal som minimum ske en sikkerhedsgodkendelse til klassifikationsgraden HEMMELIGT i overensstemmelse med sikkerhedscirkulæret.

Med den foreslåede bestemmelse sikres det, at Datarådet kan håndtere oplysninger på betryggende vis. Hvis et medlem mister sin sikkerhedsgodkendelse, vil den pågældende ikke længere kunne være medlem af rådet.

Det foreslås i lovforslagets *stk. 6* at hvervet som formand, medlem eller stedfortræder ophører ved udgangen af embedsperioden eller ved frivillig fratræden.

Det foreslås endvidere i lovforslagets *stk. 7*, at formanden, medlemmer og stedfortrædere for disse alene kan afskediges i tilfælde af alvorligt embedsmisbrug, eller hvis disse ikke længere opfylder betingelserne for at varetage hvervet.

Med de foreslåede bestemmelser understreges det, at medlemmer af Datarådet skal kunne agere uafhængigt i hele embedsperioden. Der er således ikke mulighed for at afskedige et medlem som følge af generel utilfredshed med det pågældende medlems beslutninger i Datarådet.

Der henvises i øvrigt til afsnit 2.7.3.1. i lovforslagets almindelige bemærkninger.

Det fremgår af persondatalovens § 56, at Datatilsynet varetager sine opgaver i fuld uafhængighed.

Det fremgår af forarbejderne til persondataloven (Folketingstidende 1999-2000, tillæg A, side 4101), at der ved udpegning af medlemmer af rådet skal tilstræbes uvildighed og sagkundskab, og at rådets medlemmer således skal udpeges på en måde, der sikrer Datatilsynet den fornødne uafhængighed.

Det foreslås i lovforslagets *stk. 8* at sekretariatets personale samt Datarådets formand, medlemmer og stedfortrædere for disse kun kan have bibe-skæftigelse, for så vidt og i det omfang det er foreneligt med udøvelsen af de pligter, der er knyttet til stillingen eller hvervet.

Der sker med den foreslåede bestemmelse en understregning af, at tilsynets personale og Datarådets medlemmer skal være uafhængige. Der er således i praksis tale om en videreførelse af gældende ret.

Der henvises i øvrigt til 2.7.3. i lovforslagets almindelige bemærkninger.

Det foreslås i lovforslagets *stk. 9*, at Datatilsynet repræsenterer tilsynsmyndighederne i Det Europæiske Databeskyttelsesråd.

Tilsynsmyndigheder efter loven vil være Datatilsynet og Domstolsstyrelsen. Med den foreslåede bestemmelse fastslås det, at Datatilsynet skal repræsentere tilsynsmyndighederne i Det Europæiske Databeskyttelsesråd. Datatilsynet skal i den forbindelse også varetage Domstolsstyrelsens synspunkter som tilsynsmyndighed, jf. også databeskyttelsesforordningens artikel 60 om samarbejde mellem tilsynsmyndighederne.

Til § 28

I lovforslagets § 28 foreslås det, at ved udarbejdelse af lovforslag, bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger, skal der indhentes en udtalelse fra Datatilsynet.

Det er uden betydning, om reglerne kun er bindende for ansatte i en myndighed eller tillige har retsvirkning over for borgerne. Det afgørende vil være, om reglerne har indflydelse på beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger.

Det forudsættes endvidere, at der sker høring af Datatilsynet i forbindelse med udfærdigelse af lovforslag, som fremsættes af regeringen. Endvidere forudsættes det, at vedkommende ressortministerium i forbindelse med sin stillingtagen til et privat lovforslag hører Datatilsynet.

Der skal bl.a. ske høring inden fastsættelsen af nærmere regler efter lovforslagets § 2, stk. 6-8, § 3, stk. 9, og § 5, stk. 3.

Datatilsynet skal i forbindelse med høringen udtale sig om, hvorvidt de påtænkte retsforskrifter mv. efter tilsynets opfattelse giver anledning til betænkeligheder i forhold til forordningen og denne lov eller i øvrigt i relation til beskyttelsen af de registreredes privatliv.

Hvis der i et tilfælde ikke sker høring af Datatilsynet, indebærer dette ikke, at den udstedte administrative retsforskrift er ugyldig.

Der henvises i øvrigt til afsnit 2.7.3. i lovforslagets almindelige bemærkninger.

Til § 29

Bestemmelsen i *stk. 1* afløser persondatalovens § 62, stk. 1.

Det forhold, at tilsynet kan kræve oplysninger til afgørelse af, om et forhold falder ind under lovens bestemmelser, medfører, at tilsynet bl.a. vil kunne kræve oplysninger med henblik på at afklare, om en given behandling er omfattet af undtagelsesbestemmelsen i lovforslagets § 3.

Bestemmelsen i *stk. 2* er fastsat på grundlag af forordningens artikel 58, stk. 1, litra f, hvoraf det følger, at hver tilsynsmyndighed har undersøgelsesbeføjelse til 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.

Bestemmelsen i *stk. 2*, som tager sigte på alle lokaler, hvorfra behandling af personoplysninger foretages, svarer delvist til persondatalovens § 62, stk. 2-4. Bestemmelsen giver dog på baggrund af forordningens artikel 58, stk. 1, litra f, en udvidet adgang til lokaler hos private, da forordningen ikke giver mulighed for at fastsætte bestemmelser om begrænsning af inspektionsbeføjelser svarende til persondatalovens § 62, stk. 3. For nærmere herom henvises til *betænkningen* side 807-811.

Det forudsættes i bestemmelsen, 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.

Der henvises i øvrigt til afsnit 2.7.3. i lovforslagets almindelige bemærkninger.

Til § 30

Det foreslås i *stk. 1*, at Datatilsynet afgør efter lovforslaget ikke kan indbringes for anden administrativ myndighed.

Bestemmelsen svarer til persondatalovens § 61.

Det foreslås endvidere i *stk. 2*, at tilsynsmyndighederne kan indbringe spørgsmål om overtrædelse af den foreslåede lov for retten i den borgerlige retsplejes former.

Med den foreslåede bestemmelse får tilsynsmyndighederne mulighed for at indbringe spørgsmål om overtrædelse af den foreslåede lov for domstolene i den borgerlige retsplejes former, dvs. efter retsplejelovens regler om civile sager.

Der etableres ikke med bestemmelsen en mulighed for tilsynsmyndighederne til at give møde i retten i videre omgang end efter gældende ret.

Bestemmelsen i lovforslagets § 30 er ikke til hinder for, at afgørelserne indbringes for Folketingets Ombudsmand.

Der henvises i øvrigt til afsnit 2.7.3.4. i lovforslagets almindelige bemærkninger.

Til § 31

Det følger af bestemmelsen, at hvis der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet efter artikel 45 i databeskyttelsesforordningen, kan Datatilsynet i særlige tilfælde forbyde, begrænse eller suspendere overførsel af særlige kategorier af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, til et tredjeland eller en international organisation.

Bestemmelsen er fastsat på baggrund af forordningens artikel 49, stk. 5.

Reglerne om overførsler af personoplysninger til tredjelande eller internationale organisationer er placeret i forordningens kapitel V.

Datatilsynet kan således efter forslagets § 31 forbyde, begrænse eller suspendere overførsler af oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Der henvises i øvrigt til afsnit 2.7.3. i lovforslagets almindelige bemærkninger.

§ 32

Efter lovforslagets § 32 kan Datatilsynet videregive oplysninger til tilsynsmyndigheder i andre medlemsstater i det omfang, det er nødvendigt for at påse overholdelsen af bestemmelserne i denne lov, databeskyttelsesforordningen eller den pågældende medlemsstats databeskyttelseslovgivning.

Bestemmelsen indebærer, at der vil kunne ske videregivelse til myndigheder i andre medlemsstater af oplysninger, selv om disse måtte være undergivet tavshedspligt. Det gælder dog kun i det omfang, en sådan videregivelse må anses for nødvendig.

Der henvises i øvrigt til afsnit 2.7.3. i lovforslagets almindelige bemærkninger.

§ 33

I lovforslagets § 33 foreslås det, at Datatilsynet kan offentliggøre sine udtalelser og afgørelser, ligesom bestemmelsen i lovforslagets § 22 skal finde tilsvarende anvendelse.

Efter bestemmelsen har Datatilsynet således hjemmel til at offentliggøre sine udtalelser og afgørelser. Henvisning til lovforslagets § 22 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 kendskab til oplysningerne findes at burde vige for afgørende hensyn til private og offentlige interesser. I tvivlstilfælde vil det være naturligt at indhente en udtalelse herom fra den dataansvarlige, som er part i sagen, og eventuelt tillige fra den registrerede.

Der henvises i øvrigt til afsnit 2.7.3. i lovforslagets almindelige bemærkninger.

Til § 34

Af bestemmelsen følger, at Datatilsynet samarbejder med Domstolsstyrelsen i det omfang, det er nødvendigt for at opfylde Datatilsynets pligter,

navnlig ved at udveksle alle relevante oplysninger. Tilsynsmyndigheden på domstolsområdet (Domstolsstyrelsen) skal tilsvarende samarbejde med Datatilsynet, jf. § 38, med henvisningen til § 34.

Selv om bestemmelsen er indsat i kapitlet om Datatilsynet, vil initiativet til samarbejde tilsynsmyndighederne imellem naturligvis kunne udgå fra Domstolsstyrelsen. Det forudsættes, at tilsynsmyndighederne indbyrdes drøfter spørgsmål af mere principiel karakter, således at der sker den fornødne koordinering tilsynsmyndighederne imellem. Herved sikres det, at tilsynsmyndighedernes praksis ikke udvikler sig i en forskellig retning. Det bemærkes i den forbindelse, at en række af de foreslåede bestemmelser overlader vedkommende tilsynsmyndighed et forholdsvist frit skøn ved udfyldningen af de i lovforslaget og databeskyttelsesforordningen indeholdte standarder.

Der henvises i øvrigt til afsnit 2.7.3. i lovforslagets almindelige bemærkninger.

Til § 35

Efter bestemmelsen bemyndiges justitsministeren til at fastsætte nærmere regler om, at Datatilsynet og Domstolsstyrelsen har yderligere beføjelser end dem, der er omhandlet i databeskyttelsesforordningens artikel 58, stk. 1, 2 og 3.

Det er et krav efter forordningens artikel 58, stk. 6, som giver mulighed for, at medlemsstaterne kan fastsætte yderligere beføjelser, at udøvelsen af disse beføjelser ikke må hindre en effektiv anvendelse af kapitel VII, det vil sige forordningens bestemmelser om samarbejde og sammenhæng.

Forordningens bestemmelser om samarbejde og sammenhæng skal derfor overholdes, hvis bemyndigelsen udnyttes.

Der henvises i øvrigt til afsnit 2.7.3. i lovforslagets almindelige bemærkninger.

Til § 36

Efter bestemmelsens *stk. 1* kan Datatilsynet fastsætte, at ansøgninger om tilladelser kan eller skal indgives på en bestemt måde. Dette gælder i rela-

tion til såvel den offentlige forvaltning som private. Tilsynet kan således beslutte, at der skal ansøges ved anvendelse af bestemte blanketter.

Desuden kan tilsynet bestemme, at der tillige skal ansøges ad elektronisk vej, f.eks. via e-mail eller på anden måde. Tilsynet kan efter bestemmelsen også fastsætte nærmere regler for, hvordan der kan foretages (enslydende) ansøgninger, som foretages af flere myndigheder.

Efter bestemmelsens *stk. 2* bemyndiges justitsministeren til at fastsætte nærmere regler om betaling af gebyr for indgivelse af ansøgninger om tilladelser i henhold til denne lov, herunder regler om gebyrets størrelse og om, at en tilladelse ikke meddeles, før betaling er sket.

Gebyrer vil således bl.a. kunne fastsættes, når private søger om tilladelse til behandling af følsomme oplysninger efter forordningens artikel 9, stk. 1, af hensyn til væsentlige samfundsinteresser, jf. lovforslagets § 7, stk. 4. Eller, hvis der søges om tilladelse til kreditoplysningsbureauer, advarselsregistre eller retsinformationssystemer, jf. lovforslagets § 26, stk. 1.

Efter bestemmelsens *stk. 3* bemyndiges justitsministeren til at fastsætte regler om betaling af gebyr, hvis anmodninger er åbenbart grundløse eller uforholdsmæssige, især fordi de gentages efter databeskyttelsesforordningens artikel 57, stk. 4. 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. En anmodning må på baggrund af bestemmelsens ordlyd endvidere 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. Det vil dog kun være den del af anmodning, som er uforholdsmæssig, der kan afvises eller pålægges et gebyr. Åbenbart grundløse eller uforholdsmæssige anmodninger kan endvidere afvises efter forordningens artikel 57, stk. 4. Se nærmere *betænkningen* side 783-888.

Der henvises i øvrigt til afsnit 2.7.3. i lovforslagets almindelige bemærkninger.

Til kapitel 10

Tilsyn med domstolene

Til § 37

Det fremgår af persondatalovens § 67, at Domstolsstyrelsen fører tilsyn med behandling af oplysninger, der foretages for domstolene. Tilsynet omfatter behandling af oplysninger med hensyn til domstolenes administrative forhold, jf. stk. 2.

Det fremgår endvidere af § 67, stk. 3, at for anden behandling af oplysninger træffes afgørelse af vedkommende ret. 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 foreslås i lovforslagets *stk. 1*, at Domstolsstyrelsen fører tilsyn med behandling af oplysninger, der foretages for domstolene, når disse handler uden for deres egenskab af domstol.

I bestemmelsen fastsættes det, at Domstolsstyrelsens tilsyn i det hele omfatter domstolenes administrative forhold. Domstolsstyrelsens tilsyn omfatter således den teknisk-administrative behandling af oplysninger, herunder spørgsmålet om behandlingssikkerheden. Dette indebærer bl.a., at førelsen af en elektronisk oversigt over de ved et embede ansatte personers forhold mv. er omfattet af tilsynet.

Domstolsstyrelsens tilsyn omfatter således ikke retternes judicielle funktioner.

Det foreslås endvidere i *stk. 2*, at for anden behandling af oplysninger træffes afgørelse af vedkommende ret. Afgørelsen kan kæres til højere ret. For særlige domstole, hvis afgørelser ikke kan indbringes for højere ret, kan afgørelsen kæres til den landsret, i hvis kreds retten er beliggende. Kærefristen er 4 uger fra den dag, afgørelsen er meddelt den pågældende.

Med den foreslåede bestemmelse sker der en videreførelse af gældende ret i forhold til tilsynet med domstolenes behandling af personoplysninger.

Der henvises i øvrigt til afsnit 2.7.3. i lovforslagets almindelige bemærkninger.

Til § 38

Det følger af lovforslagets *stk. 1* at for Domstolsstyrelsens udøvelse af tilsyn i henhold til § 33 gælder bestemmelserne i §§ 29 og 34. Domstolsstyrelsens afgørelser er endelige.

Efter bestemmelsen kan Domstolsstyrelsen for at udøve tilsyn således kræve enhver oplysning, der er af betydning for deres virksomhed, og Domstolsstyrelsens medlemmer og personale vil mod behørig legitimation have adgang til alle lokaler, hvorfra en behandling af personoplysninger foretages, uden retskendelse.

Endvidere skal Domstolsstyrelsen for at udøve tilsyn samarbejde med Datatilsynet i det omfang, det er nødvendigt for at opfylde Datatilsynets pligter, navnlig ved at udveksle alle relevante oplysninger.

Det forudsættes, at tilsynsmyndighederne indbyrdes drøfter spørgsmål af mere principiel karakter, således at der sker den fornødne koordinering tilsynsmyndighederne imellem. Herved sikres det, at tilsynsmyndighedernes praksis ikke udvikler sig i en forskellig retning. Det bemærkes i den forbindelse, at en række af de foreslåede bestemmelser overlader vedkommende tilsynsmyndighed et forholdsvist frit skøn ved udfyldningen af de i lovforslaget og databeskyttelsesforordningen indeholdte standarder.

Der henvises i øvrigt til afsnit 2.7.3.3. og 2.7.3.8. i lovforslagets almindelige bemærkninger.

Til § 39

Det fremgår af persondatalovens § 40, at den registrerede kan klage til vedkommende tilsynsmyndighed over behandling af oplysninger vedrørende den pågældende.

Det foreslås i *stk. 1*, at den registrerede eller dennes repræsentant kan klage til vedkommende tilsynsmyndighed over behandling af oplysninger vedrørende den registrerede.

Med den foreslåede bestemmelse videreføres den generelle adgang til at klage til tilsynsmyndigheden. Den registrerede kan klage gennem en repræsentant i overensstemmelse med forvaltningslovens regler om adgangen til at lade sig repræsentere.

Det foreslås i *stk. 2*, at tilsynsmyndighedernes afgørelser, undladelser af at behandle en klage fra en registreret eller en manglende underretning af den registrerede eller dennes repræsentant kan indbringes for domstolene efter retsplejelovens regler. Den foreslåede regel er på linje med forordningens artikel 78.

Med den foreslåede bestemmelse fastslås den registreredes adgang til at indbringe tilsynsmyndighedens afgørelser for domstolene. For så vidt angår spørgsmålet om adgangen til at indbringe en tilsynsmyndigheds afgørelser for domstolene, følger det af grundlovens § 63, at domstolene er berettiget til at påkende ethvert spørgsmål om øvrighedsmyndighedens grænser. Denne mulighed for domstolsprøvelse vil bl.a. kunne udnyttes, såfremt Datatilsynet eller Domstolsstyrelsen har behandlet en klage fra en registreret person. I givet fald vil den registrerede, som tilsynsmyndighedens afgørelse måtte gå imod, kunne indbringe denne for domstolene.

Herudover fastslås det – også på linje med forordningens artikel 78 – at den registrerede også kan indbringe tilsynsmyndigheden for domstolene, hvis der ikke er sket behandling af en klage, eller der ikke er givet den forpligtede underretning efter. Det må antages, at en sådan anlagt sag vil bortfalde, hvis tilsynsmyndigheden i mellemtiden behandler klagen eller foretager den fornødne underretning. Bestemmelsen må derfor antages at få beskeden betydning i praksis.

Det foreslås i *stk. 3*, at den registrerede eller den registreredes repræsentant kan indbringe spørgsmål om dataansvarliges og databehandlers overholdelse af denne lov for domstolene i den borgerlige retsplejes former.

Adgangen til at indbringe tilsynsmyndigheden for domstolene følger af retsplejelovens almindelige regler.

Med den foreslåede bestemmelse understreges det således, at den registrerede kan indbringe spørgsmål om dataansvarliges og databehandlers overholdelse af denne lov for retten i den borgerlige retsplejes former, dvs. efter retsplejelovens regler om civile søgsmål.

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. 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.

Der etableres ikke med bestemmelsen en mulighed for repræsentanten til at give møde i retten i videre omgang end efter gældende ret.

Der henvises i øvrigt til afsnit 2.8. i lovforslagets almindelige bemærkninger.

Til § 40

Bestemmelsen er en ordret gennemførelse af forordningens artikel 82, stk. 1. Som det fremgår af *betænkningen* side 917, udvider forordningsbestemmelsen 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 – som det fremgår samme sted i *betænkningen* – må antages at svare til gældende ret.

Derudover fastsætter forordningens artikel 82, stk. 2-3, at der fortsat gælder et præsumptionsansvar.

Det præciseres i forordningens artikel 82, stk. 4 og 5, at såfremt der er flere erstatningsansvarlige, hæfter de solidarisk med mulighed for regres.

Der henvises om forordningens artikel 82 i det hele til *betænkningen* side 910-918.

Der henvises i øvrigt til afsnit 2.8. i lovforslagets almindelige bemærkninger.

Til § 41

Det foreslås i lovforslagets § 41, at det fastsættes, hvilke bestemmelser i forordningen og loven, som er strafbelagt ved overtrædelser.

På denne baggrund foreslås det i forslagens *stk. 1*, at overtrædelser som oplistet i forordningens artikel 83, stk. 4, skal straffes med bøde eller fængsel indtil 6 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås ligeledes i forslagens *stk.* 2, at overtrædelser som oplistet i forordningens artikel 83, *stk.* 5, skal straffes med bøde eller fængsel indtil 6 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning. Herudover skal Justitsministeriet bemærke, at artikel 10 om behandling af personoplysninger vedrørende straffedomme og lovovertrædelser *også* er medtaget i oplistningen af overtrædelser, der er strafferetligt sanktioneret i bestemmelsen, jf. forslagens § 41, *stk.* 2, nr. 1.

Endvidere foreslås det i bestemmelsens *stk.* 3, at den dataansvarlige eller databehandler, der gør sig skyldig i manglende overholdelse af et påbud fra tilsynsmyndigheden, som omhandlet i databeskyttelsesforordningens artikel 58, *stk.* 2, straffes med bøde eller fængsel indtil 6 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Forslaget indebærer, at bødeniveauet med lovforslaget bør forhøjes væsentligt i forhold til det nuværende bødeniveau efter persondataloven,

Der foreslås en strafferamme på fængsel i indtil 6 måneder. Der er i den forbindelse skævet til straffelovens § 264 d, hvorefter med bøde eller fængsel indtil 6 måneder straffes den, der uberettiget videregiver meddelelser eller billeder vedrørende en andens private forhold eller i øvrigt billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget offentligheden.

Forslaget indebærer, at der vil være grundlag for, at straffen stiger til fængsel i tilfælde, hvor der f.eks. sker en forsætlig offentliggørelse af særligt beskyttelsesværdige oplysninger, såsom følsomme oplysninger i et meget betydeligt omfang.

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.

Der henvises i øvrigt til afsnit 2.8.3.7. i lovforslagets almindelige bemærkninger.

Det foreslås endvidere i bestemmelsens *stk. 4*, at databeskyttelsesforordningens artikel 83, stk. 2, skal følges ved idømmelse af straf efter forslagens stk. 1-3.

Forslaget indebærer, at der i hver enkel sag skal tage behørigt hensyn til de oplistede hensyn i artikel 83, stk. 2. Det bemærkes, at straffelovens kapitel 10 om straffens fastsættelse i øvrigt finder anvendelse.

Herudover foreslås det i bestemmelsens *stk. 6*, at databeskyttelsesrådgivere, der overtræder tavshedspligten i forslagens § 24, jf. databeskyttelsesforordningens artikel 38, stk. 5, straffes med bøde, medmindre strengere straf er forskyldt efter den øvrige lovgivning.

Der henvises i øvrigt til lovforslagets § 24, og bemærkningerne hertil.

Endvidere foreslås det i *stk. 7*, at i regler, der udstedes i medfør af loven, kan der fastsættes straf af bøde eller fængsel indtil 6 måneder. Forslaget indebærer, at der er adgang til at fastsætte strafbestemmelser i regler, der udstedes i medfør af loven, idet adgangen hertil dog fastsættes til fængsel indtil 6 måneder.

Det foreslås videre i *stk. 8*, at der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Til § 42

Det foreslås i lovforslagets § 42, *stk. 1*, at Datatilsynet bemyndiges til i sager om overtrædelse af lovforslaget, databeskyttelsesforordningen eller regler udstedt i medfør af loven at udstede administrative bødeforelæg, hvis sagerne er ukomplicerede og uden bevismæssige tvivlsspørgsmål.

Forslaget retter sig kun mod sager, hvor den dataansvarlige eller databehandleren tilstår det strafbare forhold.

Forslaget indebærer endvidere, at kompetencen er begrænset til tilfælde, hvor sagen er egnet hertil, det vil sige i ukomplicerede sager, hvor der ikke er bevismæssige tvivlsspørgsmål.

For så vidt angår sager, der kan anses for egnede til at blive afsluttet ved udstedelse af et administrativt bødeforelæg, kan nævnes sager om utilsigtet offentliggørelse af oplysninger på internettet. Sådanne sager er karakteriseret ved, at man ved en fejl er kommet til at offentliggøre oplysninger på internettet.

I tilfælde hvor den, der har begået overtrædelsen, ikke erklærer sig rede til at betale bøden inden en nærmere angivet frist, vil domstolene afgøre bødespørgsmålet. I sådanne tilfælde vil Datatilsynet skulle indgive politianmeldelse sammen med en redegørelse for tilsynsmyndighedens vurdering, herunder niveauet for bøden.

Det foreslås i bestemmelsens *stk. 2*, at retsplejelovens regler om krav til indholdet af anklageskrift og om, at en sigtet ikke er forpligtet til at udtale sig finder tilsvarende anvendelse på bødeforelæg efter denne bestemmelse.

Endelig foreslås det i bestemmelsens *stk. 3*, at såfremt bøden vedtages, bortfalder videre forfølgning. Det følger af straffuldbyrdsloven, at vedtagne bøder tillægges udpantningsret.

Der henvises i øvrigt til afsnit 2.8.3.8. i lovforslagets almindelige bemærkninger.

Til § 43

Bestemmelsen afløser persondatalovens § 71 og bestemmer, at den, der driver eller er beskæftiget med virksomhed som nævnt i lovforslagets § 26 eller som privat databehandler opbevarer personoplysninger, ved dom for strafbart forhold kan frakendes retten hertil, såfremt det udviste forhold begrunder en nærliggende fare for misbrug.

Der henvises i øvrigt til afsnit 2.8.3.9. i lovforslagets almindelige bemærkninger.

Til kapitel 13

Afsluttende bestemmelser

Til § 44

Det fremgår af persondatalovens § 72, at vedkommende minister i særlige tilfælde kan fastsætte nærmere regler for behandlinger, som udføres for den offentlige forvaltning.

Det foreslås i § 44, stk. 1, at videreføre denne adgang for vedkommende minister til i særlige tilfælde at fastsætte nærmere regler for behandlinger af personoplysninger, som udføres for den offentlige forvaltning i det omfang, det er i overensstemmelse med databeskyttelsesforordningen, og med den forskel, at det skal ske efter forhandling med justitsministeren.

Det foreslås således, at vedkommende minister efter forhandling med justitsministeren kan udstede en bekendtgørelse, hvori der kan fastsættes nærmere regler for en behandling af personoplysninger, som foretages for den offentlige forvaltning. Hvis der er tale om en behandling, som foretages for en kommunal eller regional myndighed, fastsættes reglerne af den minister, under hvis område den pågældende lovgivning hører. Inden reglerne udstedes, skal der indhentes en udtalelse fra Datatilsynet, jf. databeskyttelsesforordningens artikel 57, stk. 1, litra c.

Efter bestemmelsen kan der således fastsættes nærmere regler, som supplerer eller præciserer de *regler om behandling af personoplysninger*, der følger af databeskyttelsesforordningen eller direkte af bestemmelserne i lovforslaget, f.eks. vedrørende indsichtsretten, videregivelse af oplysninger og de sikkerhedsforanstaltninger, der knytter sig til den pågældende behandling.

Det er en forudsætning, at fastsættelsen af nærmere regler sker inden for databeskyttelsesforordningens *rammer for særregler om behandling af personoplysninger*. For nærmere om forordningens rammer for særregler kan bl.a. henvises til *betænkningen* side 161 ff. om regler for behandling af ikke-følsomme personoplysninger, side 231 ff. om regler for behandling af følsomme personoplysninger og 400 ff. om undtagelser fra den registreredes rettigheder.

Der vil således i en bekendtgørelse udstedt efter bestemmelsen kunne fastsættes regler, der begrænser den adgang til at indsamle eller videregive oplysninger, herunder følsomme oplysninger, som følger af lovforslagets eller databeskyttelsesforordningens behandlingsregler, f.eks. lovforslagets § 8 eller forordningens artikel 6 og 9.

Bestemmelsen tager – ligesom persondatalovens § 72 – sigte på behandlinger, hvor *særlige forhold* taler for, at der på bekendtgørelsesniveau fastsættes nærmere regler for behandlingen. Sådanne særlige forhold kan f.eks. være, at der i behandlingen indgår meget store mængder af følsomme oplysninger, eller at der er tale om en behandling, som indebærer en høj grad af publikumskontakt i form af henvendelser til og fra borgerne.

Det fremgår af persondatalovens § 73, at justitsministeren kan fastsætte nærmere regler for bestemte typer af behandlinger, som udføres for private dataansvarlige, herunder at bestemte typer af oplysninger ikke må behandles.

Det foreslås i § 44, stk. 2, at videreføre denne adgang for justitsministeren til at fastsætte nærmere regler for bestemte typer af behandlinger, som udføres for private dataansvarlige i det omfang, det er i overensstemmelse med databeskyttelsesforordningen.

Det foreslås således, at justitsministeren kan udstede en bekendtgørelse, hvori der kan fastsættes nærmere regler for bestemte typer af behandlinger af personoplysninger, som udføres for private dataansvarlige, herunder at bestemte typer oplysninger ikke må behandles.

Bestemmelsen giver bl.a. mulighed for at fastsætte nærmere regler for pengeinstitutters videregivelse af kreditoplysninger. Reglerne i den gældende bekendtgørelse herom (bekendtgørelse nr. 531 af 15. juni 2000) vil således kunne opretholdes i medfør af bestemmelsen i det omfang, det er i overensstemmelse med databeskyttelsesforordningen. Herudover vil det kunne præciseres, hvilke oplysninger der må indgå i bestemte behandlinger, samt hvordan de må indsamles, registreres, videregives mv.

Til § 45

Det fremgår af persondatalovens § 75, at justitsministeren kan fastsætte regler, som er nødvendige for at gennemføre de af Den Europæiske Unions udstedte beslutninger, som træffes med henblik på gennemførelse af databeskyttelsesforordningen.

Det foreslås i § 45, at justitsministeren bemyndiges til at fastsætte nødvendige administrative bestemmelser til opfyldelse af de gennemførelsesforanstaltninger, som Europa-Kommissionen måtte vedtage efter proceduren i henhold til forordningens artikel 93, jf. nærmere artikel 40, stk. 9, om ge-

nerel 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.

Af bestemmelsen følger endvidere, at justitsministeren kan fastsætte regler, som er nødvendige for at anvende de af unionens udstedte retsakter på forordningens område.

Til § 46

Det foreslås i *stk. 1*, at loven træder i kraft den 25. maj 2018.

Bestemmelsen skal ses i lyset af, at databeskyttelsesforordningen finder anvendelse – og at dansk lovgivning dermed skal være i overensstemmelse hermed – fra denne dato.

Det foreslås i *stk. 2*, at persondataloven ophæves.

Det bemærkes, at persondatalovens kapitel 6 a om behandling af personoplysninger i forbindelse med tv-overvågning i følgelovforslaget til dette lovforslag foreslås videreført i tv-overvågningsloven.

Til § 47

I medfør af den foreslåede § 26, stk. 1, nr. 1-3, videreføres tilladelsesordningen i den gældende persondatalovs § 50, stk. 1, nr. 2-3 og nr. 5.

Det foreslås i § 47, at der ikke efter ikrafttrædelse af dette lovforslag skal indhentes tilladelse, hvis der allerede inden ikrafttrædelsen er opnået tilladelse efter § 50, stk. 1, nr. 2-3 eller nr. 5, i den gældende persondatalov.

Til § 48

Bestemmelsen vedrører lovens territoriale gyldighed.

Persondataloven gælder ikke for Færøerne, jf. lovens § 83, 1. pkt., men er dog sat i kraft i medfør af denne bestemmelse ved kongelig anordning nr.

754 af 19. juni 2017 for behandling af personoplysninger for rigsmyndighederne på Færøerne. For andre end rigsmyndigheder gælder på Færøerne i stedet lagtingslov nr. 73 af 8. maj 2001 om behandling af personoplysninger med senere ændringer.

Det foreslås i *stk. 1*, at loven ikke skal gælde for Færøerne, men at loven kan sættes helt eller delvist i kraft ved kongelig anordning for rigsmyndighedernes behandling af personoplysninger med de ændringer, som de færøske forhold tilsiger.

Det bemærkes, at persondataloven som sat i kraft ved kongelig anordning nr. 754 af 19. juni 2017 for behandling af personoplysninger for rigsmyndighederne på Færøerne således forbliver sat i kraft, selvom loven ophæves i Danmark.

Persondataloven gælder endvidere ikke for Grønland, jf. lovens § 83, 2. pkt., men er sat i kraft for Grønland ved kongelig anordning nr. 1238 af 14. oktober 2016.

Det foreslås i *stk. 2*, at loven ved kongelig anordning kan sættes i kraft for Grønland – og ikke blot for rigsmyndighederne – med de afvigelser, som de grønlandske forhold tilsiger.

Det bemærkes, at persondataloven som sat i kraft for Grønland ved kongelig anordning nr. 1238 af 14. oktober 2016 således forbliver i kraft for Grønland, selv om loven ophæves i Danmark i forbindelse med gennemførelsen af dette lovforslag.