JUSTITSMINISTERIET
Lovafdelingen

Dato: 1. marts 2017
Kontor: Databeskyttelseskontoret
Sagsbeh: Kenny Rasmussen
Sagsnr.: 2016-7910-0008
Dok.: 2229227

Forslag til lov om retshåndhævende myndigheders behandling af personoplysninger[1] (gennemførelse af direktiv om databeskyttelse på retshåndhævelsesområdet)

Afsnit I

Indledende bestemmelser

Kapitel 1

Lovens område

§ 1. Loven gælder for politiets, militærpolitiets, anklagemyndighedens, herunder den militære anklagemyndigheds, kriminalforsorgens, Den Uafhængige Politiklagemyndighed og domstolenes 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, når behandlingen foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.
Stk. 2. Loven finder ikke anvendelse på den behandling af personoplysninger, som udføres for eller af politiets og forsvarets efterretningstjenester.
Stk. 3. Loven finder ikke anvendelse i forhold til behandling af personoplysninger i medfør af EU-retsakter, der den eller inden den 6. maj 2016 er

[1] Loven gennemfører Europa-Parlamentets og Rådets direktiv 2016/680/EU 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 (EU-Tidende 2016 L 119, side 89 ff.)

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

trådt i kraft på området for retligt samarbejde i straffesager og politisamarbejde, og som regulerer behandling mellem medlemsstaterne og de udpegede myndigheders adgang til EU-informationssystemer.

§ 2. Regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retstilling, går forud for reglerne i denne lov.

Kapitel 2

Definitioner

§ 3. I denne lov forstås ved:

1) Personoplysninger: Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).
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.
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.
5) Register: Enhver struktureret samling af personoplysninger, der er tilgængelig efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på funktionsbestemt eller geografisk grundlag.
6) Kompetent myndighed: Enhver offentlig myndighed eller ethvert andet organ eller enhver anden enhed, der i henhold til medlemsstaternes nationale ret er bemyndiget med hensyn til at udøve offentlig myndighed og offentlige beføjelser med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed. De kompetente myndigheder i Danmark er politiet, militærpolitiet, anklagemyndigheden, herunder den militære anklagemyndighed, kriminalforsorgen, Den Uafhængige Politiklagemyndighed og domstolene.
7) Dataansvarlig: Den kompetente myndighed, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

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, således at modtageren selvstændigt herefter træffer beslutning om, til hvilket formål og med hvilke midler denne behandler de videregivne oplysninger, uanset om det er en tredjemand eller ej. Myndigheder, som vil kunne få meddelt personoplysninger som led i en isoleret forespørgsel, betragtes ikke som modtagere.
10) Brud på persondatasikkerheden: Ethvert 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.
11) 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.
12) 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.
13) Helbredsoplysninger: Personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand.
14) International organisation: En folkeretlig organisation og organer, der er underordnet en sådan organisation, samt ethvert andet organ, der er oprettet ved eller med hjemmel i en aftale mellem to eller flere lande.

Afsnit II

Behandlingsregler

Kapitel 3

Behandling af oplysninger

§ 4. Oplysninger skal behandles i overensstemmelse med god databehandlingsskik og under hensyntagen til oplysningernes karakter.
Stk. 2. Indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, som er omfattet af § 1, stk. 1, og senere behandling må ikke være uforenelig med disse formål, jf. dog § 5.
Stk. 3. Oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.
Stk. 4. Oplysninger, som behandles, skal være korrekte og om nødvendigt ajourførte. Der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges.
Stk. 5. Den dataansvarlige træffer alle rimelige foranstaltninger til at sikre, at personoplysninger ikke videregives eller stilles til rådighed, hvis de er urigtige, ufuldstændige eller ikke ajourførte. I dette øjemed verificerer den dataansvarlige så vidt muligt kvaliteten af personoplysningerne, før de videregives eller stilles til rådighed. I forbindelse med videregivelse af oplysninger skal der så vidt muligt tilføjes nødvendige oplysninger, der gør det muligt for den modtagende kompetente myndighed at vurdere, i hvor høj grad personoplysningerne er rigtige, fuldstændige og pålidelige, og i hvilket omfang de er ajourførte. Hvis det konstateres, at der er videregivet urigtige personoplysninger, eller at personoplysninger er videregivet ulovligt, skal dette straks meddeles modtageren. Oplysningerne skal i givet fald berigtiges eller slettes eller behandlingen skal begrænses.
Stk. 6. Indsamlede oplysninger må ikke opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.
Stk. 7. Indsamlede oplysninger skal behandles på en måde, der sikrer en 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, jf. § 27.
Stk. 8. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1-7 overholdes.

§ 5. Senere behandling af oplysninger til et andet af de formål, der er nævnt i § 1, stk. 1, end det, hvortil de oprindeligt var indsamlede, kan foretages af den samme eller en anden af de kompetente myndigheder, når behandlingen sker på baggrund af lov og er nødvendig og forholdsmæssig i forhold til dette efterfølgende formål.

Stk. 2. Der kan i medfør af stk. 1 foretages behandling af oplysninger, der alene sker til arkivformål i samfundets interesse eller i historisk, statistisk eller videnskabeligt øjemed.
Stk. 3. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 og 2 overholdes.

§ 6. Når der foretages videregivelse af oplysninger, fastsætter og underretter den videregivende kompetente myndighed om eventuelle særlige vilkår for behandling af oplysninger. Der kan ikke fastsættes særlige vilkår alene som følge af, at der er tale om en videregivelse til en modtager i en anden medlemsstat.
Stk. 2. Behandling af oplysninger, der er modtaget fra en kompetent myndighed, må ikke ske i strid med særlige vilkår, som er fastsat af den videregivende kompetente myndighed.

§ 7. Den dataansvarlige skal tilrettelægge behandlingen af personoplysninger således, at der fastsættes passende frister for sletningen af personoplysninger eller regelmæssig undersøgelse af behovet for lagringen af oplysningerne. Det sikres endvidere ved proceduremæssige foranstaltninger, at tidsfristerne overholdes.

§ 8. Den dataansvarlige skal, når det er relevant, så vidt muligt sondre mellem personoplysninger om forskellige kategorier af registrerede, herunder:

1) Personer, om hvem der er væsentlig grund til at tro, at de har begået eller vil begå en strafbar handling,
2) personer, der er dømt for en strafbar handling,
3) ofre for en strafbar handling eller personer, om hvem visse faktiske omstændigheder giver anledning til at tro, at de kunne blive ofre for en strafbar handling, og
4) andre parter i forbindelse med en strafbar handling, såsom personer, der kan blive indkaldt som vidner i efterforskninger i forbindelse med strafbare handlinger eller i efterfølgende straffesager, personer, der kan tilvejebringe oplysninger om strafbare handlinger, eller kontakt- eller ledsagepersoner for de i nr. 1 og 2 omhandlede personer.

§ 9. Behandling af oplysninger må kun finde sted, når behandlingen er nødvendig for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

§ 10. Der må ikke behandles 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.
Stk. 2. Under overholdelse af betingelserne i denne lov kan der dog foretages behandling af oplysninger omfattet af stk. 1, når det er strengt nødvendigt og sker af hensyn til de formål, der er nævnt i § 1, stk. 1, herunder for at beskytte den registreredes eller en anden fysisk persons vitale interesser, eller hvis behandlingen vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede.

§ 11. Der kan træffes afgørelser, der har negativ retsvirkning for den registrerede eller betydeligt påvirker den pågældende, alene på grundlag af automatisk behandling, herunder profilering.
Stk. 2. Ved afgørelser, der er omfattet af stk. 1, skal der findes passende foranstaltninger til at sikre den registreredes berettigede interesser, herunder i det mindste en ret for den registrerede til at kræve menneskelig indgriben fra den dataansvarliges side.
Stk. 3. Justitsministeren fastsætter nærmere regler om foranstaltninger omfattet af stk. 2.

§ 12. De kompetente myndigheder skal indføre effektive mekanismer, som tilskynder til fortrolig indberetning til tilsynsmyndighederne af overtrædelser af denne lov.

Afsnit III

Den registreredes rettigheder

Kapitel 4

Oplysninger, der skal stilles til rådighed eller gives til den registrerede

§ 13. Den dataansvarlige skal stille følgende oplysninger til rådighed for den registrerede:

1) Identitet på og kontaktoplysninger for den dataansvarlige.
2) Kontaktoplysninger for databeskyttelsesrådgiveren og oplysninger om dennes funktion i forhold til de registrerede.

3) Formålene med den behandling, som personoplysningerne skal bruges til.
4) Retten til at indgive en klage til en tilsynsmyndighed og kontaktoplysningerne for tilsynsmyndigheden.
5) Den registreredes rettigheder efter kapitel 5 og 6.
6) Retten til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder i forhold til de kompetente myndigheders afgørelser om undladelse, udsættelse, begrænsning eller nægtelse efter kapitel 4-6, jf. § 40, stk. 1, nr. 9.

Stk. 2. Når det er nødvendigt for, at den registrerede kan varetage sine interesser, skal den dataansvarlige som minimum give den registrerede meddelelse om følgende:

1) Retsgrundlaget for behandlingen.
2) Det tidsrum, hvor personoplysningerne vil blive opbevaret, eller, hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum.
3) Kategorierne af eventuelle modtagere af personoplysningerne, herunder i tredjelande eller internationale organisationer.
4) Hvis det er nødvendigt, yderligere oplysninger, navnlig hvis personoplysningerne indsamles uden den registreredes vidende.

§ 14. Meddelelse efter § 13, stk. 2, kan udsættes, begrænses eller undlades, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for at

1) undgå, at der lægges hindringer i vejen for officielle eller retlige undersøgelser, efterforskninger eller procedurer,
2) undgå at skade forebyggelsen, afsløringen, efterforskningen eller retsforfølgningen af strafbare handlinger eller fuldbyrdelsen af strafferetlige sanktioner,
3) beskytte den offentlige sikkerhed,
4) beskytte statens sikkerhed, eller
5) beskytte den registreredes eller andres rettigheder.

Stk. 2. Justitsministeren fastsætter nærmere regler om, hvilke kategorier af behandling der er omfattet af stk. 1, samt om, at meddelelse efter § 13, stk. 2, kan udsættes til et passende tidspunkt, for så vidt hensynene i stk. 1 må antages at medføre, at meddelelser i almindelighed må underkastes en sådan udsættelse.

Kapitel 5

Den registreredes indsigtsret

§ 15. Fremsætter en registreret begæring herom, skal den dataansvarlige bekræfte over for den pågældende, om der behandles oplysninger om vedkommende.

Stk. 2. Behandles der oplysninger om den pågældende, skal der gives adgang til oplysningerne samt en meddelelse med følgende oplysninger:

1) Formålene med og retsgrundlaget for behandlingen.
2) De berørte kategorier af personoplysninger.
3) De modtagere eller kategorier af modtagere, som personoplysningerne er videregivet til, navnlig modtagere i tredjelande eller internationale organisationer.
4) Om muligt, det påtænkte tidsrum, hvor personoplysningerne vil blive opbevaret, eller, hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum.
5) Retten til at anmode den dataansvarlige om berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede.
6) Retten til at indgive en klage til tilsynsmyndigheden og kontaktoplysningerne for tilsynsmyndigheden.
7) Hvilke personoplysninger, der er omfattet af behandlingen, og enhver tilgængelig oplysning om, hvorfra de stammer.

§ 16. Indsigt efter § 15 kan udsættes, begrænses eller nægtes, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for de hensyn til offentlige interesser, der er nævnt i § 14, stk. 1.

Stk. 2. En afgørelse om, at den registreredes indsigt udsættes, begrænses eller nægtes skal meddeles den registrerede skriftligt og skal være ledsaget af en begrundelse og en klagevejledning. Afgørelsen skal endvidere indeholde oplysninger om den registreredes ret til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder, jf. § 40, stk. 1, nr. 9.

Stk. 3. Af hensyn til de i stk. 1 nævnte formål kan den registrerede i stedet for meddelelse efter stk. 2 gives meddelelse om, at det ikke kan oplyses, om der behandles oplysninger om den pågældende. En sådan meddelelse skal indeholde en klagevejledning og oplysninger om den registreredes ret til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder, jf. § 40, stk. 1, nr. 9.

Stk. 4. Justitsministeren fastsætter nærmere regler om, hvilke kategorier af behandling der er omfattet af stk. 1, herunder om undtagelser fra retten til at få oplysninger efter § 15 for så vidt hensynene i stk. 1 må antages at medføre, at begæringer om indsigt i almindelighed må nægtes.

Kapitel 6

Ret til berigtigelse, sletning og begrænsning af behandling

§ 17. Den dataansvarlige skal efter anmodning fra den registrerede uden unødig forsinkelse berigtige oplysninger, der viser sig urigtige. På tilsvarende måde skal der ske fuldstændiggørelse af ufuldstændige oplysninger, hvis dette kan ske uden at bringe formålet med behandlingen i fare. Den dataansvarlige skal meddele berigtigelse af urigtige personoplysninger til den kompetente myndighed, hvorfra de urigtige oplysninger stammer.

Stk. 2. Den dataansvarlige skal efter anmodning fra den registrerede uden unødig forsinkelse slette oplysninger, der er behandlet i strid med kapitel 3, eller hvis det er påkrævet for at overholde en retlig forpligtelse, som den dataansvarlige er underlagt.

Stk. 3. Den dataansvarlige skal i stedet for berigtigelse efter stk. 1 eller sletning efter stk. 2 begrænse behandlingen af personoplysninger, hvis:

1) Rigtigheden af personoplysningerne bestrides af den registrerede og deres rigtighed eller urigtighed ikke kan konstateres, eller
2) personoplysningerne skal bevares som bevismiddel.

Stk. 4. Hvis behandling er begrænset i henhold til stk. 3, nr. 1, underretter den dataansvarlige den registrerede herom, inden begrænsningen af behandling ophæves.

Stk. 5. Et afslag på en anmodning om berigtigelse, sletning eller begrænsning af behandling skal meddeles den registrerede skriftligt og skal være ledsaget af en begrundelse og en klagevejledning. Afgørelsen skal endvidere indeholde oplysninger om den registreredes ret til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder, jf. § 40, stk. 1, nr. 9. Bestemmelsen i § 16, stk. 3, finder tilsvarende anvendelse.

Stk. 6. Den dataansvarlige skal underrette modtagere om, at der er sket berigtigelse, sletning eller begrænsning af behandling af personoplysninger. Modtagerne berigtiger eller sletter personoplysningerne eller begrænser behandling af personoplysninger, som de har ansvaret for.

Kapitel 7

Generelle bestemmelser

§ 18. Oplysninger og meddelelser, der er nævnt i dette afsnit, skal stilles til rådighed eller gives gratis, i en kortfattet, letforståelig og lettilgængelig form og i et klart og enkelt sprog.
Stk. 2. Den dataansvarlige skal snarest og på skrift besvare begæringer som nævnt i dette afsnit. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om hvornår anmodningen forventes besvaret.
Stk. 3. Når personoplysninger er indeholdt i en retsafgørelse eller et register, der er knyttet til udstedelsen af en retsafgørelse, skal anmodninger i medfør af dette afsnit gennemføres i henhold til retsplejelovens regler.

§ 19. Den dataansvarlige kan afvise at imødekomme åbenbart grundløse eller overdrevent gentagne anmodninger, som er fremsat i henhold til bestemmelserne i dette afsnit.

Afsnit IV

Forpligtelser for den dataansvarlige og databehandleren

Kapitel 8

Forpligtelser for den dataansvarlige

§ 20. Den dataansvarlige gennemfører og om nødvendigt ajourfører og reviderer de fornødne tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne lov. Hvis det står i rimeligt forhold til behandlingsaktiviteterne, skal den dataansvarlige tillige gennemføre de fornødne databeskyttelsespolitikker.
Stk. 2. Foranstaltninger efter stk. 1 omfatter databeskyttelse gennem design og gennem standardindstillinger.

§ 21. Hvis to eller flere dataansvarlige i fællesskab fastsætter formålene med og hjælpemidlerne til behandling, betragtes de som fælles dataansvarlige. Fælles dataansvarlige skal fastsætte en ordning for fordeling af ansvaret for, at behandlingen er i overensstemmelse med loven, herunder navnlig i forhold til den registreredes rettigheder efter kapitel 5-7. Ordningen skal omfatte udpegningen af et fælles kontaktpunkt. Der kan udpeges et særligt kontaktpunkt, der kan fungere som fælles kontaktpunkt for de registrerede, når disse udøver deres rettigheder.

Kapitel 9

Forpligtelser for databehandleren mv.

§ 22. Når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 20 og § 24 nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.

Stk. 2. Gennemførelse af en behandling ved en databehandler skal ske i henhold til lov eller en skriftlig aftale mellem databehandleren og den dataansvarlige. Loven eller aftalen skal fastsætte genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder. Det skal navnlig fremgå, at databehandleren

1) kun må handle efter instruks fra den dataansvarlige,
2) sikrer, at de fysiske personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt,
3) bistår den dataansvarlige på enhver hensigtsmæssig måde med at sikre overholdelse af bestemmelserne om den registreredes rettigheder,
4) efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysningerne til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, medmindre anden lovgivning foreskriver opbevaring af personoplysningerne,
5) stiller alle oplysninger, der er nødvendige for at påvise overholdelse af denne bestemmelse, til rådighed for den dataansvarlige, og
6) overholder betingelserne i stk. 2 og 3 med henblik på at gøre brug af en anden databehandler.

Stk. 3. En databehandlers overladelse af behandling til en anden databehandler skal ske i henhold til en generel eller specifik skriftlig aftale med den dataansvarlige. Sker overladelse i henhold til en generel aftale, skal databehandleren underrette den dataansvarlige herom senest 14 dage forud for overladelsen.

Stk. 4. Enhver, der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, må kun behandle disse oplysninger efter instruks fra den dataansvarlige, medmindre det følger af anden lovgivning, at den pågældende skal foretage behandlingen.

Kapitel 10

Fortegnelser over behandlingsaktiviteter og logning

§ 23. Den dataansvarlige skal føre skriftlige fortegnelser over alle kategorier af behandlingsaktiviteter under den dataansvarliges ansvar. Fortegnelserne skal indeholde følgende oplysninger:

1) Navn på og kontaktoplysninger for den dataansvarlige og, hvis det er relevant, den fælles dataansvarlige og databeskyttelsesrådgiveren,
2) formålene med behandlingen,
3) de kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, herunder modtagere i tredjelande eller internationale organisationer,
4) en beskrivelse af kategorierne af registrerede og kategorierne af personoplysninger,
5) hvor det er relevant, brugen af profilering,
6) hvor det er relevant, kategorierne af overførsler af personoplysninger til et tredjeland eller en international organisation,
7) en angivelse af retsgrundlaget for behandlingsaktiviteten, herunder overførsler, hvortil personoplysningerne er bestemt,
8) hvis det er muligt, de forventede tidsfrister for sletning af de forskellige kategorier af personoplysninger, og
9) hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i § 27.

Stk. 2. Databehandleren fører skriftlige fortegnelser over alle kategorier af behandlingsaktiviteter, der foretages på vegne af en dataansvarlig. Fortegnelserne skal indeholde følgende oplysninger:

1) Navn på og kontaktoplysninger for databehandleren eller databehandlerne, for hver dataansvarlig, på hvis vegne databehandleren handler, samt, hvis det er relevant, databeskyttelsesrådgiveren,
2) de kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige,
3) hvor det er relevant, overførsler af personoplysninger til et tredjeland eller en international organisation, når den dataansvarlige udtrykkeligt har givet instruks herom, herunder angivelse af dette tredjeland eller denne internationale organisation, og
4) hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i § 27.

§ 24. I automatiske databehandlingssystemer foretages logning af indsamling, ændring, søgning, videregivelse, herunder overførsel, samkøring og sletning.
Stk. 2. Justitsministeren fastsætter nærmere regler om, hvilke automatiske databehandlingssystemer der er omfattet af stk. 1.

Kapitel 11

Konsekvensanalyser og høring af tilsynsmyndighederne

§ 25. 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, skal den dataansvarlige forud for behandlingen foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger.
Stk. 2. Analysen skal indeholde en generel beskrivelse af de planlagte behandlingsaktiviteter, en vurdering af risiciene for de registreredes rettigheder, de foranstaltninger, der påtænkes for at imødegå disse risici, garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af denne lov, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

§ 26. Den dataansvarlige eller databehandleren skal høre tilsynsmyndigheden inden behandling af personoplysninger, der vil indgå som en del af et nyt register, der skal oprettes, når

1) en konsekvensanalyse vedrørende databeskyttelse, jf. § 25, viser, at behandlingen vil føre til en høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen, eller
2) den type behandling, navnlig ved brug af nye teknologier, mekanismer eller procedurer, indebærer en høj risiko for de registreredes rettigheder.

Stk. 2. Finder tilsynsmyndigheden, at den planlagte behandling ikke vil overholde loven, herunder navnlig hvis den dataansvarlige ikke tilstrækkeligt har identificeret eller begrænset risikoen, giver tilsynsmyndigheden inden for en periode på op til 6 uger efter modtagelse af anmodningen om høring den dataansvarlige og, hvor det er relevant, databehandleren skriftlig rådgivning. Tilsynsmyndigheden kan i den forbindelse anvende enhver af sine beføjelser, jf. kapitel 20. Denne periode kan forlænges med en måned under hensyntagen til den påtænkte behandlings kompleksitet. Til-

synsmyndigheden 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.
Stk. 3. Tilsynsmyndighederne fastsætter en liste over de behandlingsaktiviteter, hvor der i henhold til stk. 1 skal foretages en forudgående høring.

Afsnit V

Personoplysningssikkerhed

Kapitel 12

Behandlingssikkerhed

§ 27. Den dataansvarlige og databehandleren skal under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og behandlingens karakter, omfang, sammenhæng og formål samt risicienes varierende sandsynlighed og alvor for fysiske personers rettigheder gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, navnlig for så vidt angår behandlingen af de særlige kategorier af personoplysninger, der er omfattet af § 10.
Stk. 2. For så vidt angår automatisk behandling, skal den dataansvarlige eller databehandleren på grundlag af en risikovurdering gennemføre foranstaltninger til at sikre, at

1) uautoriserede personer ikke kan få adgang til det behandlingsudstyr, der benyttes til behandling (kontrol med fysisk adgang til udstyret),
2) der ikke sker uautoriseret læsning, kopiering, ændring eller sletning af datamedier (kontrol med datamedier),
3) der ikke sker uautoriseret indlæsning af personoplysninger samt uautoriseret læsning, ændring eller sletning af opbevarede personoplysninger (kontrol med opbevaring),
4) automatiske behandlingssystemer ikke via datakommunikationsudstyr kan benyttes af uautoriserede personer (brugerkontrol),
5) personer med bemyndigelse til at anvende et automatisk behandlingssystem kun har adgang til de personoplysninger, der er omfattet af deres adgangstilladelse (kontrol med dataadgangen),

6) det er muligt at kontrollere og fastslå de modtagere, til hvilke der er blevet eller kan transmitteres eller stilles oplysninger til rådighed ved hjælp af datakommunikationsudstyr (kommunikationskontrol),
7) det er muligt efterfølgende at undersøge og fastslå, hvilke personoplysninger der er indlæst i automatiske behandlingssystemer, og hvornår og af hvem personoplysningerne blev indlæst (kontrol med indlæsning),
8) der ikke sker uautoriseret læsning, kopiering, ændring eller sletning af personoplysninger i forbindelse med overførsler af disse eller under transport af datamedier (transportkontrol), og
9) de anvendte systemer i tilfælde af teknisk uheld kan genetableres (genopretning), og
10) systemet fungerer, at indtrufne fejl meldes (pålidelighed), og at opbevarede personoplysninger ikke bliver ødelagt som følge af fejlfunktioner i systemet (integritet).

Stk. 3. For oplysninger af særlig interesse for fremmede magter skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold, jf. dog stk. 5.

Stk. 4. Justitsministeren fastsætter nærmere regler om de i stk. 1-3 nævnte foranstaltninger.

Stk. 5. Justitsministeren kan efter indstilling fra en kompetent myndighed fastsætte regler om, at det er ufornødent, at personoplysninger omfattet af stk. 3, underlægges foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse, hvis dette ud fra en samlet vurdering må anses for forsvarligt.

Kapitel 13

Brud på datasikkerheden

§ 28. Ved brud på persondatasikkerheden skal den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet, anmelde bruddet til tilsynsmyndigheden, medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder. En overskridelse af fristen på 72 timer skal begrundes.

Stk. 2. Databehandleren underretter uden unødig forsinkelse den dataansvarlige om et brud på persondatasikkerheden.

Stk. 3. Anmeldelsen efter stk. 1 skal:

1) beskrive karakteren af bruddet på persondatasikkerheden, herunder i videst muligt omfang kategorierne og det berørte antal

registrerede samt kategorierne og det berørte antal registreringer af personoplysninger,

2) angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes,
3) beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden, og
4) 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.

Stk. 4. Når det ikke er muligt at forelægge oplysningerne, der er nævnt i stk. 3, samlet for tilsynsmyndigheden, skal oplysningerne meddeles trinvis uden unødig forsinkelse.

Stk. 5. Den dataansvarlige skal dokumentere alle brud på persondatasikkerheden, som er omfattet af stk. 1, herunder de faktiske omstændigheder vedrørende bruddet, dets virkninger og de trufne afhjælpende foranstaltninger.

Stk. 6. Hvis bruddet på persondatasikkerheden omhandler oplysninger, der er transmitteret af eller til en dataansvarlig i en anden medlemsstat, skal oplysninger, der er nævnt i stk. 3, uden unødig forsinkelse meddeles til den dataansvarlige i denne medlemsstat.

§ 29. Ved brud på persondatasikkerheden, som sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder, skal den dataansvarlige uden unødig forsinkelse underrette den registrerede om bruddet.

Stk. 2. Underretningen skal i et klart og enkelt sprog beskrive karakteren af bruddet samt indeholde de oplysninger, der er nævnt i § 28, stk. 3, nr. 2-4.

Stk. 3. Bestemmelsen i stk. 1 gælder ikke, hvis

1) 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 f.eks. på grund af kryptering gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil,
2) den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder som omhandlet i stk. 1 sandsynligvis ikke længere er reel, eller
3) det vil kræve en uforholdsmæssig indsats af den dataansvarlige. I et sådant tilfælde skal der i stedet foretages en offentlig med-

delelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

Stk. 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.

Stk. 5. Underretning af den registrerede kan udsættes, begrænses eller undlades af de grunde, der er nævnt i § 14, stk. 1.

Afsnit VI

Databeskyttelsesrådgiver

Kapitel 14

Udpegelse af databeskyttelsesrådgiver

§ 30. Den dataansvarlige udpeger på grundlag af faglige kvalifikationer, herunder navnlig ekspertise inden for databeskyttelsesret og -praksis samt evnen til at udføre de opgaver, der er nævnt i kapitel 15, en databeskyttelsesrådgiver, som inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger.

Stk. 2. Flere dataansvarlige kan under hensyntagen til deres størrelse og organisatoriske forhold udpege en fælles databeskyttelsesrådgiver.

Stk. 3. Bestemmelsen i stk. 1 gælder ikke for domstolene, når disse foretager behandling af personoplysninger inden for deres egenskab af domstole.

Stk. 4. Den dataansvarlige offentliggør kontaktoplysningerne for databeskyttelsesrådgiveren og meddeler disse til tilsynsmyndigheden.

Kapitel 15

Databeskyttelsesrådgiverens stilling og opgaver

§ 31. Den dataansvarlige understøtter, at databeskyttelsesrådgiveren kan

1) underrette og rådgive den dataansvarlige og de ansatte, der behandler personoplysninger, om deres forpligtelser i medfør af denne lov og anden lovgivning om databeskyttelse,
2) overvåge overholdelsen af denne lov og anden lovgivning om databeskyttelse og af den dataansvarliges politikker om beskyttelse af personoplysninger, herunder fordeling af ansvar, oplys-

ningskampagner og uddannelse af det personale, der medvirker ved behandlingsaktiviteterne, og de tilhørende revisioner,

3) rådgive, når der anmodes herom, med hensyn til konsekvensanalysen vedrørende databeskyttelse og overvåge dens opfyldelse i henhold til bestemmelsen i § 25,
4) samarbejde med tilsynsmyndigheden, og
5) fungere som tilsynsmyndighedens kontaktpunkt i spørgsmål vedrørende behandling, herunder den forudgående høring, der er nævnt i § 26, og at høre tilsynsmyndigheden, når det er hensigtsmæssigt, om eventuelle andre spørgsmål.

Afsnit VII

Overførsler af personoplysninger til tredjelande eller internationale organisationer

Kapitel 16

Generelle principper

§ 32. Overførsel af personoplysninger, der behandles eller planlægges behandlet efter overførsel til et tredjeland eller en international organisation, herunder videreoverførsel til et andet tredjeland eller en anden international organisation, må kun finde sted under overholdelse af reglerne i denne lov, og hvis betingelserne i dette afsnit er overholdt, herunder navnlig at

1) overførslen er nødvendig i forhold til de formål, der er nævnt i § 1, stk.1,
2) personoplysningerne overføres til en dataansvarlig i et tredjeland eller en international organisation, der er en myndighed, der er kompetent i forhold til de formål, der er nævnt i § 1, stk.1,
3) hvor personoplysninger transmitteres eller stilles til rådighed af en kompetent myndighed fra en anden medlemsstat, denne myndighed har givet sin forudgående godkendelse til overførslen i henhold til dens nationale regler,
4) der foreligger et af de overførselsgrundlag, der er nævnt i kapitel 17, og
5) den kompetente myndighed, der foretog den oprindelige overførsel, i tilfælde af videreoverførsel til et andet tredjeland eller en anden international organisation, giver bemyndigelse til videreoverførslen, efter at den har taget behørigt hensyn til alle

relevante faktorer, herunder den strafbare handlings grovhed, det formål, hvortil personoplysningerne oprindeligt blev overført, og beskyttelsesniveauet for personoplysninger i det tredjeland eller den internationale organisation, hvortil personoplysningerne videreoverføres.

Stk. 2. Overførsel uden forudgående godkendelse efter stk. 1, nr. 3, kan ske, hvis overførslen er nødvendig for at forebygge en umiddelbar og alvorlig trussel mod en medlemsstats eller et tredjelands offentlige sikkerhed eller mod en medlemsstats væsentlige interesser, og den forudgående godkendelse ikke kan indhentes i tide. Den myndighed, der er ansvarlig for at give den pågældende godkendelse, underrettes straks om overførslen.

Kapitel 17

Grundlag for overførsel

§ 33. Overførsel kan ske, hvis Europa-Kommissionen har truffet afgørelse om, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation har et tilstrækkeligt beskyttelsesniveau.

§ 34. Foreligger der ikke en afgørelse som nævnt i § 33, kan der ske overførsel, hvis

1) der er givet de fornødne garantier, hvad angår beskyttelsen af personoplysninger, i en international aftale, eller
2) den dataansvarlige har vurderet alle forhold i forbindelse med overførslen af personoplysninger og konkluderer, at der findes de fornødne garantier, for beskyttelsen af personoplysninger.

Stk. 2. Den dataansvarlige underretter tilsynsmyndigheden om kategorier af overførsler i medfør af stk. 1, nr. 2.

Stk. 3. En overførsel i medfør af stk. 1, nr. 2, dokumenteres i forhold til dato og tidspunkt for overførslen, oplysninger om den modtagende kompetente myndighed, begrundelsen for overførslen og de overførte personoplysninger. Dokumentationen stilles efter anmodning til rådighed for tilsynsmyndigheden.

§ 35. Foreligger der ikke en afgørelse som nævnt i § 33 eller de fornødne garantier som nævnt i § 34, kan en overførsel eller en kategori af overførsler kun finde sted, hvis overførslen er nødvendig

1) for at beskytte den registreredes eller en anden persons vitale interesser,

2) for at beskytte den registreredes legitime interesser, hvis det er fastsat i henhold til lov,
3) for at afværge en umiddelbar og alvorlig trussel mod en medlemsstats eller et tredjelands offentlige sikkerhed,
4) i enkeltsager med henblik på de formål, der er nævnt i § 1, stk. 1, eller
5) i en enkeltsag for, at retskrav kan fastlægges, gøres gældende eller forsvares med henblik på de formål, der er nævnt i § 1, stk. 1.

Stk. 2. Overførsel efter stk. 1, nr. 4 og 5, kan ikke finde sted, hvis hensynet til den registreredes rettigheder går forud for den samfundsmæssige interesse i overførslen.

Stk. 3. En overførsel i medfør af stk. 1 dokumenteres i forhold til dato og tidspunkt for overførslen, oplysninger om den modtagende kompetente myndighed, begrundelsen for overførslen og de overførte personoplysninger. Dokumentationen stilles efter anmodning til rådighed for tilsynsmyndigheden.

§ 36. De kompetente myndigheder kan overføre personoplysninger til andre end kompetente myndigheder og internationale organisationer på baggrund af international aftale eller i enkeltstående og specifikke tilfælde, hvis

1) overførslen er strengt nødvendig for den overførende kompetente myndigheds udførelse af en af lovgivningen følgende opgave og forfølger de formål, der er nævnt i § 1, stk. 1,
2) den overførende kompetente myndighed fastslår, at ingen af den pågældende registreredes grundlæggende rettigheder går forud for samfundets interesse, der nødvendiggør overførslen i det foreliggende tilfælde,
3) den overførende kompetente myndighed mener, at overførslen til en myndighed, der i tredjelandet er kompetent i forhold til de formål, der er nævnt i § 1, stk.1, er ineffektiv eller uhensigtsmæssig, navnlig fordi overførslen ikke kan foretages i tide,
4) den myndighed, der i tredjelandet er kompetent i forhold til de formål, der er nævnt i § 1, stk. 1, underrettes uden unødig forsinkelse, medmindre dette er ineffektivt eller uhensigtsmæssigt, og
5) den overførende kompetente myndighed underretter modtageren om det eller de specifikke formål, hvortil sidstnævnte udelukkende kan behandle personoplysningerne, forudsat at denne behandling er nødvendig.

Stk. 2. Den overførende kompetente myndighed dokumenterer og underretter tilsynsmyndigheden om overførsler i medfør af stk. 1.

Afsnit VIII

Tilsynsmyndighed

Kapitel 18

Datatilsynet

§ 37. Datatilsynet, der består af et råd og et sekretariat, fører tilsyn med enhver behandling, der omfattes af loven, jf. dog kapitel 19.
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 6 andre medlemmer. Der kan udpeges 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, herunder navnlig ekspertise inden for databeskyttelsesret.
Stk. 4. Rådet fastsætter sin forretningsorden og de nærmere regler om arbejdets fordeling 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 til stillingen eller hvervet knyttede pligter.
Stk. 9. Datatilsynet repræsenterer tilsynsmyndighederne i Det Europæiske Databeskyttelsesråd.

Kapitel 19

Tilsyn med domstolene

§ 38. Domstolsstyrelsen fører tilsyn med behandling af oplysninger, der foretages for domstolene, når disse handler uden for 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 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.

Kapitel 20

Tilsynsmyndighedernes opgaver og beføjelser

§ 39. Tilsynsmyndighederne udøver deres funktioner i fuld uafhængighed.

§ 40. Tilsynsmyndighederne har til opgave her i landet at

1) føre tilsyn med og håndhæve anvendelsen af denne lov,
2) fremme offentlighedens kendskab til og forståelse af risici, regler, garantier og rettigheder i forbindelse med behandling af personoplysninger,
3) rådgive Folketinget, regeringen og andre institutioner og organer om lovgivningsmæssige og administrative foranstaltninger til beskyttelse af fysiske personers rettigheder i forbindelse med behandling,
4) fremme dataansvarliges og databehandleres kendskab til deres forpligtelser i medfør af denne lov,
5) efter anmodning informere alle registrerede om udøvelsen af deres rettigheder i medfør af denne lov og med henblik herpå samarbejde med tilsynsmyndighederne i andre medlemsstater, hvis det er relevant,
6) behandle klager, der indgives af en registreret eller af et organ, en organisation eller en sammenslutning i overensstemmelse med bestemmelsen i § 48, og, for så vidt det er hensigtsmæssigt, undersøge genstanden for klagen og underrette klageren om forløbet og resultatet af undersøgelsen inden for senest 3 måneder, navnlig hvis yderligere undersøgelse eller koordinering med en anden tilsynsmyndighed er nødvendig,
7) efter anmodning yde supplerende bistand til en registreret, der har indgivet en klage,

8) underrette en registreret, der har indgivet en klage, om adgangen til retsmidler efter kapitel 22,
9) efter anmodning kontrollere, om en behandling af personoplysninger er lovlig i henhold til undladelse, udsættelse, begrænsning eller nægtelse efter kapitel 4-6, og underrette den registrerede inden for en rimelig frist om resultatet af undersøgelsen eller om årsagerne til, at undersøgelsen ikke er foretaget, og om den registreredes adgang til retsmidler efter kapitel 22,
10) samarbejde med andre tilsynsmyndigheder, herunder gennem udveksling af oplysninger og gensidig bistand med henblik på at sikre ensartet anvendelse og håndhævelse af denne lov,
11) gennemføre undersøgelser om anvendelsen af denne lov, herunder på grundlag af oplysninger, der er modtaget fra en anden tilsynsmyndighed eller en anden offentlig myndighed,
12) holde øje med relevant udvikling, for så vidt den har indvirkning på beskyttelse af personoplysninger, navnlig udviklingen for informations- og kommunikationsteknologi,
13) rådgive om behandlingsaktiviteter som omhandlet i § 26, og
14) bidrage til Databeskyttelsesrådets aktiviteter.

Stk. 2. Tilsynsmyndighederne fastsætter nærmere regler for at lette indgivelsen af klager efter stk. 1, nr. 6.

Stk. 3. Tilsynsmyndighederne kan afvise at imødekomme åbenbart grundløse eller overdrevent gentagne anmodninger efter denne lov.

§ 41. Tilsynsmyndighederne kan kræve enhver oplysning, der er af betydning for deres virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

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

§ 42. Tilsynsmyndighederne kan over for den dataansvarlige og databehandleren afgive udtalelse om, at planlagte behandlingsaktiviteter sandsynligvis vil være i strid med denne lov, give påbud om at bringe behandlingsaktiviteter i overensstemmelse med denne lov, eller midlertidigt eller definitivt begrænse, herunder forbyde, behandling af personoplysninger.

Stk. 2. Tilsynsmyndighedernes afgørelser efter denne lov kan ikke indbringes for anden administrativ myndighed.

§ 43. Ved udarbejdelse af generelle retsforskrifter, der har betydning for behandling af personoplysninger, skal der indhentes en udtalelse fra Data-

tilsynet. Hvis der er tale om generelle forskrifter, der har betydning for behandling af oplysninger, der foretages for domstolene, skal der indhentes en udtalelse fra Domstolsstyrelsen.

§ 44. Tilsynsmyndighederne kan indbringe spørgsmål om overtrædelser af denne lov for retten i den borgerlige retsplejes former.

§ 45. Tilsynsmyndighederne afgiver en årlig beretning om deres virksomhed til Folketinget og justitsministeren. Beretningerne offentliggøres.

Kapitel 21

Samarbejde

§ 46. Tilsynsmyndighederne samarbejder, i det omfang det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle relevante oplysninger.

§ 47. Tilsynsmyndighederne besvarer anmodninger fra en tilsynsmyndighed i en anden medlemsstat uden unødig forsinkelse og senest en måned efter modtagelsen. Oplysninger, som en tilsynsmyndighed i en anden medlemsstat har anmodet om, fremsendes elektronisk i et standardformat.
Stk. 2. 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.
Stk. 3. Anmodninger kan alene afvises, når den anmodede tilsynsmyndighed ikke har kompetence med hensyn til genstanden for anmodningen eller de foranstaltninger, som den anmodes om at iværksætte, eller en imødekommelse af anmodningen vil være i strid med denne eller anden lov. Et afslag på at imødekomme en anmodning skal begrundes.

Afsnit IX

Retsmidler, ansvar og sanktioner

Kapitel 22

Retsmidler, ansvar og sanktioner

§ 48. Den registrerede eller dennes repræsentant kan klage til vedkommende tilsynsmyndighed over behandling af oplysninger vedrørende den registrerede.
Stk. 2. Tilsynsmyndighedernes afgørelser, undladelser af at behandle en klage fra en registreret eller en manglende underretning efter § 40, stk. 1, nr. 6, kan af den registrerede eller dennes repræsentant indbringes for domstolene i den borgerlige retsplejes former.
Stk. 3. Den registrerede eller dennes repræsentant kan indbringe spørgsmål om dataansvarliges og databehandleres overholdelse af denne lov for domstolene i den borgerlige retsplejes former.

§ 49. Enhver person, som har lidt materiel eller immateriel skade som følge af en ulovlig behandlingsaktivitet eller enhver anden behandling i strid med denne lov, har ret til erstatning fra den dataansvarlige i overensstemmelse med de almindelige erstatningsretlige principper.

§ 50. Medmindre højere straf er forskyldt efter anden lovgivning, kan en privat databehandler, der i forbindelse med en behandling, der udføres for en kompetent myndighed, overtræder § 22, stk. 2 og 3, § 23, stk. 2, § 27 og § 28, stk. 2, eller undlader at efterkomme et påbud eller forbud, der er meddelt i henhold til § 42, straffes med bøde eller fængsel indtil 4 måneder.
Stk. 2. Dataansvarlige, der undlader at efterkomme et påbud eller forbud, der er meddelt i henhold til § 42, straffes med bøde.
Stk. 3. I regler, der udstedes i medfør af loven, kan der fastsættes straf af bøde eller fængsel indtil 4 måneder.
Stk. 4. Der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Afsnit X

Afsluttende bestemmelser

Kapitel 23

Afsluttende bestemmelser, herunder ikrafttrædelsesbestemmelser mv.

§ 51. Justitsministeren kan fastsætte regler, som er nødvendige for at gennemføre de af Europa-Kommissionen udstedte retsakter, som træffes med henblik på gennemførelse af direktivet 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, eller regler, som er nødvendige for at anvende de af Europa-Kommissionen udstedte retsakter på direktivets område.

§ 52. Loven træder i kraft dagen efter bekendtgørelse i Lovtidende.
Stk. 2. Lovforslaget kan stadfæstes straks efter dets vedtagelse.

§ 53. Lovens §§ 25 og 26 gælder i forhold til ny behandling af personoplysninger, der iværksættes, og registre, der oprettes, den 1. maj 2017 eller senere.
Stk. 2. Lovens § 20, stk. 2, gælder i forhold til automatiske databehandlingssystemer, der idriftsættes den 1. maj 2017 eller senere.

§ 54. Overførsler til tredjelande og internationale organisationer kan ske i medfør af internationale aftaler, der er indgået inden den 6. maj 2016, indtil de ændres, erstattes eller ophæves.

§ 55. I lov nr. 429 af 31. maj 2000 om behandling af personoplysninger, som senest ændret ved lov nr. 639 af 12. juni 2013, foretages følgende ændringer:

1. *§ 2, stk. 4,* ophæves. Stk. 5-11 bliver herefter til stk. 4-10.

2. Efter § 2 indsættes i *kapitel 1*:

»**§ 2 a.** Loven gælder ikke for behandling, som er omfattet af lov om retshåndhævende myndigheders behandling af personoplysninger, jf. dog stk. 2.

Stk. 2. Regler udstedt i medfør af § 32, stk. 5, § 41, stk. 5, § 55, stk. 4, og § 72 gælder for den behandling af personoplysninger, der er omfattet af lov om retshåndhævende myndigheders behandling af personoplysninger. Reglerne gælder ikke, hvis det vil være i strid med denne lov.«

§ 56. Loven gælder ikke for Færøerne, men kan ved kongelig anordning sættes i kraft for rigsmyndighedernes behandling af oplysninger med de afvigelser, som de færøske forhold tilsiger. Loven gælder heller ikke for Grønland, men kan ved kongelig anordning sættes i kraft med de afvigelser, som de grønlandske forhold tilsiger.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

1.1. Formål og baggrund

Lovforslaget gennemfører Europa-Parlamentets og Rådets direktiv 2016/680/EU 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 (retshåndhævelsesdirektivet). Direktivet er medtaget som bilag til dette lovforslag.

Retshåndhævelsesdirektivet er vedtaget under henvisning til artikel 16, stk. 2, i Traktaten om den Europæiske Unions Funktionsmåde (TEUF), og da det fastsætter regler vedrørende medlemsstaternes behandling af personoplysninger under udøvelse af aktiviteter, der er omfattet af det danske forbehold vedrørende retlige og indre anliggender, er direktivet ikke bindende for og finder ikke anvendelse i Danmark, jf. artikel 2 og 2 a i protokollen om Danmarks stilling.

Da direktivet er en udbygning af Schengenreglerne, kan Danmark imidlertid i henhold til protokollens artikel 4 inden 6 måneder efter Rådets vedtagelse træffe afgørelse om, at Danmark vil gennemføre direktivet i dansk ret. Træffer Danmark afgørelse om, at direktivet skal gennemføres i dansk ret, skabes der en folkeretlig forpligtelse mellem Danmark og de øvrige medlemsstater, der er bundet af retshåndhævelsesdirektivet.

Folketinget meddelte ved beslutning af 25. oktober 2016 sit samtykke til, at regeringen tilsluttede sig retshåndhævelsesdirektivet, hvilket regeringen meddelte Rådet den 26. oktober 2016.

Hertil kommer, at gennemførslen af direktivet inden 1. maj 2017 skal ses i lyset af, at gennemførslen er en forudsætning for, at der kan indgås en samarbejdsaftale mellem Danmark og Europol, som skal have virkning fra samme dato.

Det bemærkes, at regeringen vil søge Folketingets samtykke efter grundlovens § 19 til, at Danmark indgår aftale om fortsat tilknytning til Europol, i forbindelse med det kommende lovforslag om ændring af lov om Den Europæiske Politienhed (Europol).

Lovforslaget skal endvidere ses i lyset af det sideløbende arbejde med at sikre, at dansk ret er i overensstemmelse med Europa-Parlamentets og Rådets forordning 2016/679/EU 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 (databeskyttelsesforordningen).

Databeskyttelsesforordningen, som finder anvendelse i medlemsstaterne fra den 25. maj 2018, udgør sammen med retshåndhævelsesdirektivet en

samlet databeskyttelsespakke. Forordningen og direktivet er imidlertid sammenfaldende på visse områder, f.eks. hvad angår kravene til tilsynsmyndighederne. Arbejdet med at sikre, at dansk ret er i overensstemmelse med forordningen pågår, og der vil blive fremsat selvstændigt lovforslag herom.

Henset til, at gennemførslen af retshåndhævelsesdirektivet inden 1. maj 2017 er en forudsætning for dansk tilknytning til Europol efter denne dato, har Justitsministeriet fundet, at gennemførslen af retshåndhævelsesdirektivet bør ske selvstændigt.

Justitsministeriet har endvidere fundet, at gennemførslen af retshåndhævelsesdirektivet i videst muligt omfang bør ske i en samlet lov, der omfatter databehandling for de kompetente danske myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed. Denne fremgangsmåde varetager både hensynet til at sikre en korrekt implementering af direktivet og skaber en højere grad af overskuelighed for de myndigheder, som vil skulle anvende lovgivningen. Denne tilgang fører samtidig til, at der skal ske en ændring af persondatalovens anvendelsesområde, således at de kompetente myndigheders behandling af personoplysninger ikke længere er omfattet af persondataloven, når den er omfattet af lovforslagets anvendelsesområde.

Affattelsen af de foreslåede regler er generelt lagt tæt op ad retshåndhævelsesdirektivets ordlyd, idet hensynet til at sikre, at der ikke kan rejses tvivl om implementeringen af direktivets bestemmelser efter Justitsministeriets opfattelse taler herfor.

1.2. Lovforslagets indhold i hovedtræk

Lovforslaget er inddelt i afsnit om henholdsvis indledende bestemmelser, herunder anvendelsesområdet og definitioner (afsnit I), behandlingsregler (afsnit II), den registreredes rettigheder (afsnit III), forpligtelser for den dataansvarlige og databehandleren (afsnit IV), personoplysningssikkerhed (afsnit V), databeskyttelsesrådgiveren (afsnit VI), overførsler til tredjelande eller internationale organisationer (afsnit VII), tilsynsmyndigheder (afsnit VIII), retsmidler, ansvar og sanktioner (afsnit IX) og afsluttende bestemmelser, herunder ikrafttrædelsesbestemmelser (afsnit X).

Lovforslagets regler er i nogen grad en videreførelse af de gældende regler for de retshåndhævende myndigheder.

For så vidt angår *anvendelsesområdet*, skal de foreslåede regler gælde for behandling af personoplysninger, som foretages af politiet, militærpolitiet, anklagemyndigheden, herunder den militære anklagemyndighed, kriminalforsorgen, Den Uafhængige Politiklagemyndighed, og domstolene med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

For så vidt angår lovforslagets *behandlingsregler*, er der i vidt omfang tale om en videreførelse af de gældende regler, idet der dog indføres enkelte yderligere principper om tidsfrister for opbevaring af personoplysninger og revision af behovet herfor, ligesom der foreslås eksplicitte regler om sondring mellem forskellige kategorier af registrerede og personoplysninger samt kontrol med kvaliteten af personoplysninger.

For så vidt angår lovforslagets regler om den *registreredes rettigheder*, herunder retten til information, indsigt, berigtigelse og sletning, er der tale om en udvidelse af rettighederne i forhold til gældende ret om behandling af personoplysninger på det strafferetlige område. Dette skyldes, at de gældende regler i persondataloven om oplysningspligt over for den registrerede, den registreredes ret til indsigelse, berigtigelse, blokering og sletning af personoplysninger ikke finder anvendelse på behandlinger, der foretages for domstolene, politi og anklagemyndighed inden for det strafferetlige område. Herudover finder de gældende regler om den registreredes ret til indsigt ikke anvendelse på behandlinger, der foretages for domstolene inden for det strafferetlige område.

I forhold til lovforslagets regler om den *dataansvarliges og databehandlerens forpligtelser*, herunder pligten til at udpege en *databeskyttelsesrådgiver*, er der tale om en række nyskabelser. Således vil den dataansvarlige – med undtagelse af domstolene, når disse foretager behandling af personoplysninger inden for deres egenskab af domstole – efter den foreslåede ordning som noget nyt være forpligtet til at udpege en databeskyttelsesrådgiver, som skal inddrages i spørgsmål om databeskyttelse.

Endvidere skal den dataansvarlige forud for behandling af personoplysninger, der indebærer en høj risiko for fysiske personers rettigheder, foretage

konsekvensanalyser og i visse tilfælde foretage en forudgående høring af tilsynsmyndigheden.

En anden nyskabelse er den foreslåede indførelse af et krav om, at den dataansvarlige uden unødig forsinkelse under visse omstændigheder skal anmelde brud på persondatasikkerheden, som sandsynligvis vil medføre en risiko for fysiske personers rettigheder, til tilsynsmyndigheden og – i visse tilfælde – underrette den registrerede.

Der sker endvidere med lovforslaget en ændring af de gældende krav til logning. I overensstemmelse med direktivet foreslås det imidlertid, at spørgsmålet om, hvilke automatiske databehandlingssystemer, som logningskravet skal finde anvendelse på, håndteres efterfølgende i en bekendtgørelse med henblik på, at der kan ske en nærmere afklaring af logningsforpligtelsens omfang.

For så vidt angår lovforslagets regler om *overførsler til tredjelande eller internationale organisationer*, er der i nogen grad tale om en videreførelse af de gældende regler, idet sådanne overførsler kan ske på baggrund af en afgørelse fra Europa-Kommissionen om, at tredjelandet mv. sikrer et tilstrækkeligt beskyttelsesniveau.

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 de retshåndhævende myndigheders behandling af personoplysninger

1.3.1. Persondataloven

I lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer (persondataloven) er der fastsat generelle regler om behandling af personoplysninger for offentlige myndigheder, herunder rets-

håndhævende myndigheder, med undtagelse af politiets og forsvarets efterretningstjenester (PET og FE).

Persondataloven er først og fremmest baseret på Europa-Parlamentets 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 (databeskyttelsesdirektivet).

Persondataloven indeholder bl.a. regler om, hvornår behandling af personoplysninger i almindelighed må finde sted, ligesom loven indeholder regler vedrørende behandling af særlige typer oplysninger (f.eks. regler om personnumre).

Persondataloven gælder generelt for de kompetente myndigheders behandling af personoplysninger. Lovens bestemmelser om oplysningspligt over for den registrerede, og om den registreredes ret til indsigelse, berigtigelse, blokering og sletning af personoplysninger finder dog ikke anvendelse på behandlinger, der foretages for domstolene, politiet og anklagemyndigheden inden for det strafferetlige område. Herudover finder lovens regler om den registreredes ret til indsigt ikke anvendelse på behandlinger, der foretages for domstolene inden for det strafferetlige område.

Persondataloven fastsætter endvidere regler om datasikkerhed i forbindelse med behandling af personoplysninger, hvorefter den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger bl.a. ikke kommer til uvedkommendes kendskab.

1.3.2. Bekendtgørelse om beskyttelse af personoplysninger i forbindelse med internationalt politisamarbejde og retligt samarbejde i kriminalsager

Justitsministeren har i medfør af persondatalovens § 72 a fastsat nærmere regler ved bekendtgørelse nr. 1287 af 25. november 2010 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager inden for Den Europæiske Union og Schengensamarbejdet (rammeafgørelsesbekendtgørelsen).

Bekendtgørelsen gennemfører Rådets rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager (rammeafgørelsen) i dansk ret.

Bekendtgørelsen finder anvendelse i forhold til personoplysninger, der udveksles eller stilles til rådighed mellem en dansk og en udenlandsk myndighed i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager inden for EU og Schengen-samarbejdet.

Bekendtgørelsen tager således sigte på den grænseoverskridende informationsudveksling i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager.

Bekendtgørelsen henviser bl.a. til en række af de grundlæggende regler for behandling af personoplysninger i persondataloven. Den indeholder herudover regler om datakvalitet og behandlingssikkerhed. Bekendtgørelsen indeholder desuden regler for specifikke former for databehandling, herunder regler om viderebehandling af personoplysninger modtaget fra andre medlemsstater og om videregivelse af sådanne oplysninger til private og tredjelande samt internationale organer.

Herudover udvider bekendtgørelsen den registreredes rettigheder med hensyn til bl.a. underretning og berigtigelse af urigtige oplysninger i forhold til persondataloven.

1.3.3. Retsplejeloven

Retsplejeloven (lovbekendtgørelse nr. 1257 af 13. oktober 2016) indeholder de grundlæggende regler i dansk ret vedrørende bl.a. efterforskning og retsforfølgning af strafbare forhold.

Retsplejelovens kapitel 67-75 b fastsætter således regler om politiets efterforskning af strafbare forhold og om gennemførelsen af tvangsindgreb, herunder reglerne for anholdelse, varetægtsfængsling, indgreb i meddelelseshemmeligheden, legemsindgreb, ransagning, beslaglæggelse, edition og personundersøgelser. Disse kapitler indeholder ligeledes grundlæggende straffeprocessuelle regler.

Retsplejeloven indeholder endvidere regler om aktindsigt i domme, kendelser og andre dokumenter, der vedrører en straffesag. Udgangspunktet er, at enhver har ret til aktindsigt i domme og kendelser mv., ligesom den, der har en individuel, væsentlig interesse i et konkret retsspørgsmål, som udgangspunkt kan forlange at blive gjort bekendt med dokumenter, der vedrører en straffesag, herunder indførsler i retsbøgerne, i det omfang dokumenterne har betydning for vurderingen af det pågældende retsspørgs-

mål. Herudover indeholder retsplejeloven regler om berigtigelse af retsafgørelser.

Herudover er der i retsplejelovens § 115 bl.a. fastsat regler om, hvornår politiet kan udveksle oplysninger om enkeltpersoners rent private forhold til andre myndigheder som led i bl.a. det kriminalitetsforebyggende samarbejde (SSP-samarbejdet).

1.3.4. Straffuldbyrdelsesloven

Straffuldbyrdelsesloven (lovbekendtgørelse nr. 1242 af 11. november 2015 med senere ændringer) regulerer fuldbyrdelsen af fængselsstraffe, bødestraffe, betingede domme, domme med vilkår om samfundstjeneste og forvaring.

Straffuldbyrdelsesloven indeholder mulighed for, at myndighederne i en række tilfælde kan behandle personoplysninger om en dømt person for at varetage deres opgaver efter loven.

Det er f.eks. tilfældet, hvor kriminalforsorgen træffer afgørelse om valg af afsoningsinstitution, herunder om anbringelse i åbent eller lukket fængsel, om overførsel fra åbent til lukket fængsel og om udgang i forbindelse med afsoning af fængselsstraf.

1.3.5. Politiloven

Politiloven (lovbekendtgørelse nr. 956 af 20. august 2015 om politiets virksomhed) indeholder bestemmelser om politiets formål og virke samt politiets opgaver. Endvidere indeholder loven bestemmelser om politiets indgreb, herunder i forhold til orden og sikkerhed, offentlige forsamlinger og opløb samt svage og udsatte persongrupper. Loven regulerer herudover politiets anvendelse af magt og betingelserne for brug af særlige magtmidler samt politiets adgang til at lade foranstaltninger udføre som selvhjælpshandlinger.

Politiloven forudsætter i en række tilfælde, at politiet foretager behandling af personoplysninger som led i varetagelsen af de opgaver, der er henlagt til politiet efter loven. Det kan f.eks. være i forbindelse med gennemførelsen af legemsbesigtigelse, frihedsberøvelser, opgaver knyttet til offentlige forsamlinger og opløb, detentionsanbringelser og anvendelse af magtmidler.

2. Lovforslagets hovedpunkter

2.1. Anvendelsesområde

2.1.1. Gældende ret

2.1.1.1. Databeskyttelsesdirektivet finder ikke anvendelse på medlemsstaternes aktiviteter på det strafferetlige område, jf. artikel 3, stk. 2.

Den generelle EU-retlige regulering af beskyttelse af personoplysninger på det politi- og strafferetlige område findes i rammeafgørelsen, jf. pkt. 1.3.2.

Rammeafgørelsen finder anvendelse, når der med henblik på at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner udveksles eller er udvekslet personoplysninger mellem medlemsstater (enten i form af videregivelse af personoplysninger eller ved at personoplysninger stilles eller er stillet til rådighed for en anden medlemsstat), jf. artikel 1.

Rammeafgørelsen finder endvidere anvendelse, når personoplysninger udveksles eller er udvekslet mellem på den ene side kompetente myndigheder i medlemsstaterne og på den anden side organer eller informationssystemer inden for EU-samarbejdet, jf. artikel 1, stk. 2.

Rammeafgørelsen tager således sigte på den grænseoverskridende informationsudveksling i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, og den finder inden for dette område anvendelse på behandling af personoplysninger, der helt eller delvis foretages elektronisk, samt på ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, jf. artikel 1, stk. 3.

Rammeafgørelsen berører ikke væsentlige nationale sikkerhedsinteresser og specifikke efterretningsaktiviteter vedrørende national sikkerhed, jf. artikel 1, stk. 4.

2.1.1.2. Persondataloven gælder generelt for behandling af personoplysninger, der 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, jf. lovens § 1, stk. 1. Regler om behandling

af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i persondataloven, jf. § 2, stk. 1.

Persondataloven gælder således også for de kompetente myndigheders behandling af personoplysninger.

Det fremgår imidlertid af lovens § 2, stk. 4, at lovens bestemmelser om oplysningspligt over for den registrerede (kapitel 8), den registreredes ret til indsigelse, berigtigelse, blokering og sletning af personoplysninger (§§ 35-37) og om automatiske afgørelser (§ 39) ikke finder anvendelse på behandlinger, der foretages for domstolene, politiet og anklagemyndigheden inden for det strafferetlige område. Herudover finder lovens regler om den registreredes ret til indsigt (kapitel 9) ikke anvendelse på behandlinger, der foretages for domstolene inden for det strafferetlige område.

Det antages, at begrebet "det strafferetlige område" i denne bestemmelses forstand skal defineres bredt. Begrebet omfatter i hvert fald kerneområdet af domstolenes samt politiets og anklagemyndighedens virksomhed inden for strafferetsplejen, dvs. behandling af traditionelle sager, som er under efterforskning, eller hvor der tages stilling til strafansvar og strafudmåling. Udover dette kerneområde, er det i praksis antaget, at også politiets og anklagemyndighedens aktiviteter af mere generel karakter på det strafferetlige område kan være omfattet af begrebet.

I medfør af persondataloven har Datatilsynet således bl.a. fundet, at de behandlingsaktiviteter, der er knyttet til politiets brug af automatisk nummerpladegenkendelse (ANPG) og til brugen af meddelere, faldt inden for det strafferetlige område, uanset at der ikke er tale om aktiviteter i tilknytning til en konkret straffesag.

2.1.2. Retshåndhævelsesdirektivet

Det fremgår af retshåndhævelsesdirektivets artikel 2, at direktivet finder anvendelse på kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

Det fremgår videre af direktivets artikel 2, stk. 2, at direktivet finder anvendelse på behandling af personoplysninger, der helt eller delvist foretages ved hjælp af automatisk databehandling, og på anden ikke-automatisk

behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Det fremgår herudover af direktivets artikel 2, stk. 3, at direktivet ikke finder anvendelse på behandling af personoplysninger under udøvelse af aktiviteter, der falder uden for EU-retten, og på behandling foretaget af EU-institutioner, -organer, -kontorer og -agenturer.

Det fremgår af direktivets præambelbetragtning nr. 12, at de aktiviteter, der udføres af politiet eller andre retshåndhævende myndigheder, hovedsageligt er fokuseret på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger, herunder politiaktiviteter uden forudgående viden om, hvorvidt et forhold udgør en strafbar handling eller ej. Sådanne aktiviteter kan også omfatte udøvelsen af beføjelser gennem tvangsindgreb som f.eks. politiaktiviteter i forbindelse med demonstrationer, store sportsbegivenheder og uroligheder. De omfatter også opretholdelse af lov og orden som en opgave, der er overdraget til politiet eller andre retshåndhævende myndigheder, hvor det er nødvendigt for at beskytte mod og forebygge trusler mod den offentlige sikkerhed og de ved lov beskyttede grundlæggende samfundsinteresser, som kan føre til en strafbar handling.

Endeligt fremgår det af direktivets artikel 1, stk. 3, at direktivet ikke er til hinder for, at medlemsstaterne fastsætter højere standarder for beskyttelse af den registreredes rettigheder. Der er med andre ord tale om et minimumsharmoniseringsdirektiv.

2.1.3. Justitsministeriets overvejelser og lovforslagets udformning

2.1.3.1. Ved fastlæggelsen af retshåndhævelsesdirektivets anvendelsesområde bør det holdes for øje, at baggrunden for, at der blev foreslået og vedtaget en særskilt retsakt om de kompetente myndigheders behandling af personoplysninger til brug for varetagelsen af opgaver knyttet til det strafferetlige område, er en følge af de særlige hensyn, der gør sig gældende på dette område, jf. herved den i pkt. 1.1 beskrevne sammenhæng med databeskyttelsesforordningen. I erklæring nr. 21 om beskyttelse af personoplysninger inden for retligt samarbejde i straffesager og politisamarbejde, der er knyttet som bilag til slutakten fra den regeringskonference, der vedtog Lissabontraktaten, erkendte konferencen således, at det kunne blive nødvendigt med specifikke regler om beskyttelse af personoplysninger og om fri bevægelighed for personoplysninger inden for retligt samarbejde i

straffesager og politisamarbejde baseret på artikel 16 i TEUF som følge af disse områders specifikke karakter.

Retshåndhævelsesdirektivet er udtryk for, at der som angivet i ovennævnte erklæring er fundet behov for at udforme særligt tilpassede regler for de kompetente myndigheders behandling af personoplysninger til brug for løsningen af visse opgaver, hvilket bl.a. indebærer, at en række af de krav til behandlingen af personoplysninger, rettigheder for de registrerede mv., som er fastsat i den generelle databeskyttelsesforordning, jf. punkt 1.1 ovenfor, ikke indgår i retshåndhævelsesdirektivet. Hertil kommer, at valget af at regulere området ved et direktiv – frem for ved en forordning, der er almengyldig, bindende i alle enkeltheder og umiddelbart gyldig i hver medlemsstat – indebærer, at der i udgangspunktet overlades medlemsstaterne et større råderum.

Retshåndhævelsesdirektivets anvendelsesområde kan opdeles i forskellige elementer. Således angår afgræsningen af anvendelsesområdet for det første spørgsmålet om, hvorvidt der kræves et grænseoverskridende element, og for det andet, hvilke former for behandling af personoplysninger der er omfattet.

Anvendelsesområdet afgrænses for det tredje af, hvilke myndigheder der er omfattet, og for det fjerde af, hvilket formål behandlingen af personoplysninger har. Endeligt afgrænses anvendelsesområdet for det femte af EU-rettens generelle anvendelsesområde.

2.1.3.2. For så vidt angår spørgsmålet om, hvorvidt der stilles krav om et grænseoverskridende element, er anvendelsesområdet for retshåndhævelsesdirektivet, jf. artikel 2, bredere end for rammeafgørelsen, som alene finder anvendelse på den grænseoverskridende informationsudveksling i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager inden for EU og Schengen-samarbejdet.

Retshåndhævelsesdirektivet finder således anvendelse på både den grænseoverskridende og den rent nationale behandling af personoplysninger. Det foreslås på den baggrund, at lovforslagets anvendelsesområde på dette punkt udformes i overensstemmelse hermed.

2.1.3.3. Retshåndhævelsesdirektivet finder ligesom persondataloven og databeskyttelsesdirektivet anvendelse på behandling af personoplysninger, der helt eller delvist foretages ved hjælp af automatisk databehandling, og

på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, jf. artikel 2, stk. 2. Det foreslås på den baggrund, at lovforslagets anvendelsesområde på dette punkt udformes i overensstemmelse hermed.

2.1.3.4. For så vidt angår spørgsmålet om, hvilke myndigheder retshåndhævelsesdirektivet finder anvendelse på, fremgår det af direktivets artikel 2, at der skal være tale om *kompetente myndigheders* behandling af personoplysninger.

De kompetente retshåndhævende myndigheder defineres i direktivets artikel 3, nr. 7, som enhver offentlig myndighed, der er kompetent med hensyn til at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

Definitionen er således knyttet til forståelsen af begrebet "strafbare handlinger", jf. pkt. 2.1.3.5 nedenfor. Det fremgår af direktivets præambelbetragtning nr. 13, at en strafbar handling er et selvstændigt EU-retligt begreb som fortolket af EU-Domstolen.

Det fremgår af EU-Domstolens praksis, at der i forhold til spørgsmålet om, hvorvidt en foranstaltning skal betragtes som en straf, skal lægges vægt på de såkaldte Engels-kriterier, som er fastlagt af Den Europæiske Menneskerettighedsdomstol i forhold til spørgsmålet om, hvorvidt en foranstaltning skal betragtes som en straf omfattet af Den Europæiske Menneskerettighedskonventions artikel 6, jf. bl.a. dom af 8. juni 1976 (i sagen Engels m.fl. mod Nederlandene), hvor Menneskerettighedsdomstolen anførte, at der skal lægges vægt på, hvorvidt de bestemmelser, der udgør grundlaget for forfølgningen, i det pågældende (nationale) retssystem henregnes til strafferetten eller anses for at være af disciplinærretlig, forvaltningsretlig eller anden ikke-strafferetlig karakter. Der skal endvidere lægges vægt på karakteren af den pågældende forseelse, navnlig om der er tale om overtrædelser af forskrifter, der påhviler bestemte persongrupper, eller overtrædelser af almene normer, der gælder for enhver. Endelig skal der lægges vægt på karakteren og intensiteten af den sanktion, der kan blive tale om at ikende. Den faktisk ikendte sanktion er således ikke i sig selv afgørende.

I dansk retspleje er det et grundlæggende princip, at bøder og fængselsstraffe har karakter af strafferetlige sanktioner, som kun kan pålægges ved

domstolene og efter retsplejelovens regler, dvs. som et led i strafferetsplejen. Denne procedure sikrer borgernes retssikkerhed, idet domstolsprocessen sikrer en effektiv beskyttelse af den sigtede.

Justitsministeriet finder på den baggrund, at de "kompetente myndigheder" i direktivets forstand i en dansk kontekst skal udgøres af de myndigheder, som varetager opgaver inden for strafferetsplejen, dvs. politiet, militærpolitiet, anklagemyndigheden, herunder den militære anklagemyndighed, kriminalforsorgen, Den Uafhængige Politiklagemyndighed og domstolene (de kompetente myndigheder).

Lovforslagets anvendelsesområde på dette punkt foreslås udformet i overensstemmelse hermed.

Denne afgrænsning af anvendelsesområdet indebærer, at andre myndigheders behandling af oplysninger fra de kompetente myndigheder, f.eks. kommunernes behandling af oplysninger fra politiet som led i kriminalitetsforebyggende samarbejde (SSP-samarbejdet), ikke vil være omfattet af loven, uanset at også *kommunernes* behandling i princippet er dækket af lovens anvendelsesområde, f.eks. fordi behandlingen har forebyggelse af kriminalitet som formål. Tilsvarende vil gælde den behandling af personoplysninger, som foretages af f.eks. Arbejdstilsynet, Finanstilsynet og Fødevarestyrelsen som led i udstedelsen af administrative bødeforelæg, idet sådanne sager overgives til politiet, hvis de pågældende ikke ønsker at vedtage bødeforelægget, hvorefter sagen håndteres inden for strafferetsplejen.

Disse myndigheders behandling af personoplysninger vil i stedet være omfattet af de generelle regler i persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen.

2.1.3.5. For så vidt angår spørgsmålet om afgræsningen af anvendelsesområdet i forhold til, hvilket formål behandlingen af personoplysninger har, fremgår det af direktivets artikel 2, stk. 1, jf. artikel 1, stk. 1, at direktivet finder anvendelse på behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge *strafbare handlinger* eller fuldbyrde *strafferetlige sanktioner*, herunder beskytte mod eller forebygge trusler med den offentlige sikkerhed.

Spørgsmålet om, til hvilket formål behandlingen skal foregå, hænger således til dels sammen med det ovenfor anførte om afgræsningen i forhold til

de kompetente myndigheder og de særlige hensyn, der ligger bag beslutningen om at underlægge området særskilte databeskyttelsesretlige regler. Der skal således være tale om aktiviteter, der knytter sig til strafbare handlinger, hvilket som nævnt ovenfor i en dansk kontekst er de aktiviteter, som er omfattet af strafferetsplejen.

Mere specifikt er det Justitsministeriets vurdering, at de forseelser, der i en dansk kontekst kan føre til en bøde eller fængselsstraf, udgør "strafbare handlinger" i direktivets forstand. Det skyldes, at der er tale om overtrædelser af generelle retsforskrifter, hvor forfølgningen håndteres i det straffeprocessuelle system. Hertil kommer, at en manglende betaling af en bøde i princippet fører til en forvandlingsstraf i form af fængsel, jf. straffelovens § 53.

Direktivet finder imidlertid også anvendelse på aktiviteter, som ikke er knyttet til en helt konkret strafbar handling. Det fremgår således af præambelbetragtning nr. 12, der uddyber definitionen på en kompetent myndighed i artikel 3, nr. 7, at direktivet omfatter politiaktiviteter, der finder sted uden forudgående viden om, hvorvidt et forhold udgør en strafbar handling eller ej. Direktivet omfatter således også politiaktiviteter, der retter sig mod potentielle strafbare forhold, hvilket er et område, der under dansk ret generelt henføres under politiets ordenshåndhævelsesbeføjelser. Herudover fremgår det af direktivets præambelbetragtning nr. 12, at direktivet også omfatter udøvelsen af beføjelser gennem *tvangsindgreb* som f.eks. politiaktiviteter i forbindelse med demonstrationer, store sportsbegivenheder og uroligheder. De omfatter også opretholdelse af lov og orden som en opgave, der er overdraget til politiet eller andre retshåndhævende myndigheder, hvor det er nødvendigt for at *beskytte mod og forebygge trusler mod den offentlige sikkerhed* og de ved lov beskyttede grundlæggende samfundsinteresser, *som kan føre til en strafbar handling*.

Anvendelsesområdet knytter sig således også til *forebyggelse* af strafbare handlinger, hvilket må antages at omfatte generelle forebyggelsesindsatser, f.eks. i forhold til færdselskontrol, som ikke – endnu – har forbindelse til konkrete strafbare forhold. Således vil direktivet også omfatte f.eks. de i pkt. 2.1.1.2 nævnte behandlingsaktiviteter, der er knyttet til politiets brug af automatisk nummerpladegenkendelse (ANPG) og til brugen af meddelere, uanset at der ikke er tale om aktiviteter i tilknytning til en konkret straffesag.

Rækkevidden af direktivets anvendelsesområde i forhold til kriminalforsorgens opgaver på straffuldbyrdelses- og forebyggelsesområdet skal forstås således, at kriminalforsorgens resocialiseringsindsatser, programvirksomhed (anger management, voldsforebyggelse mv.), misbrugsbehandling og uddannelse er omfattet af direktivet. Almindelige forsorgsopgaver i forhold til de indsatte mv., som f.eks. behandling af oplysninger i forbindelse med administration af mad, lønninger eller gejstlig betjening vil også være omfattet.

Behandling af helbredsoplysninger er omfattet af direktivets anvendelsesområde i det omfang, at behandlingen har til formål at fuldbyrde strafferetlige sanktioner eller forebygge kriminalitet, hvilket f.eks. vil omfatte behandling af helbredsoplysninger ved lægetilsyn i forbindelse med magtanvendelse og anbringelse i sikringscelle samt psykiske evalueringer eller diagnosticeringer til brug for vurdering af f.eks. afsoningssted. Behandling af helbredsoplysninger til andre formål, f.eks. almindelige helbredsfaglige behandlinger som rensning af sår, diagnosticering, administration af medicin mv., vil derimod falde uden for direktivets anvendelsesområde.

Der vil endvidere være tale om de aktiviteter, som de kompetente myndigheder udøver med henblik på at beskytte den offentlige sikkerhed i konkrete situationer, f.eks. i forbindelse større varslede og uvarslede hændelser, samt den mere generelle løbende overvågning af konkrete objekter, der vurderes at være mulige mål for sikkerhedstrusler mv.

Spørgsmålet om rækkevidden af direktivets anvendelsesområde i forhold til politiets opgaver forbundet med opretholdelse af lov og orden vil dog skulle fastlægges nærmere i praksis, idet de kompetente myndigheders varetagelse af deres opgaver ikke i alle tilfælde entydigt falder inden for eller uden for dette område. Det må dog kunne lægges til grund, at de dele af politiets ordenshåndhævelse, der finder sted gennem brug af tvangsindgreb og som i øvrigt har som umiddelbart sigte at forebygge eller forhindre trusler mod den offentlige orden, er omfattet af direktivet. Endvidere vil politiets dispositioner knyttet til ordenshåndhævelse – der generelt må antages at finde sted uden forudgående viden om, hvorvidt et forhold udgør en strafbar handling eller ej – også anses for at være omfattet af direktivets anvendelsesområde.

Derimod vil politiets behandling af f.eks. klager over politiets dispositioner – såvel inden for som uden for strafferetsplejen – der finder sted under iagttagelse af generelle forvaltningsretlige regler, ikke kunne siges at ved-

røre strafbare forhold eller ordensmæssige forhold, og vil derfor ikke være omfattet af direktivet. Eksempelvis vil politiets besøg og besigtigelse af konkrete virksomheder, der udøver virksomhed i henhold til konkrete tilladelser, f.eks. kampsportsstævner, ikke være at anse som opgaver forbundet med opretholdelse af lov og orden i direktivets forstand, desuagtet at kontrollen udøves af det uniformerede politi.

De kompetente myndigheder behandler en række andre administrative sager. Politiet behandler f.eks. sager om tilladelser til udøvelse af forskellige hverv, herunder pantelånere, idrætskontrollører, dørmænd og vagter, samt tilladelser til afholdelse af forskellige offentlige arrangementer eller aktiviteter, herunder forlystelser og særtransporter. Ligeledes modtager og behandler politiet og andre retshåndhævende myndigheder, som andre forvaltningsmyndigheder, løbende aktindsigtsanmodninger efter offentlighedsloven og forvaltningsloven og vil også fremadrettet skulle behandle personoplysninger i forbindelse med behandlingen af konkrete anmodninger om indsigt i henhold til den gældende databeskyttelsesretlige regulering.

Administrative sager af denne art kan ikke antages at have en sådan karakter, der kan føre til, at behandlingen af personoplysninger i disse sager er omfattet af direktivets anvendelsesområde.

På tilsvarende måde vil behandling af personoplysninger, der finder sted i forbindelse med de kompetente myndigheders ansættelse af medarbejdere og den løbende administration af ansættelsesmæssige forhold falde uden for direktivets anvendelsesområde.

Behandling af personoplysninger i sådanne sager vil i stedet være omfattet af de generelle regler i persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen.

I forhold til politiets behandling af personlysninger i forbindelse med varetagelsen af opgaver forbundet med grænsekontrol, kan den del af grænsekontrollen, der udøves med henblik på umiddelbart at fastslå, om en person har lovligt indrejse- og opholdsgrundlag, ikke anses for at være omfattet af direktivets anvendelsesområde. Dette skyldes, at formålet med den behandling af personoplysninger, der finder sted som led i den umiddelbare grænsekontrol, ikke vedrører aktuelle eller potentielle strafbare forhold eller håndhævelsen af lov og orden i direktivets forstand. Derimod vil f.eks. politiets eventuelle kontrol af, om den pågældende måtte være efter-

søgt af danske eller udenlandske myndigheder med henblik på at fastslå, om den pågældende skal tilbageholdes mv., indebære en behandling af personoplysninger med henblik på at understøtte politiets arbejde med at forebygge, retsforfølge mv. strafbare forhold og dermed falde inden for direktivets anvendelsesområde.

Det bemærkes, at de fælleseuropæiske regelsæt på dette område ofte indeholder specifikke databeskyttelsesretlige særregler, der i relevant omfang vil skulle iagttages parallelt med direktivets – og dermed lovens – regler.

Lovforslagets anvendelsesområde foreslås udformet i overensstemmelse hermed.

2.1.3.6. Retshåndhævelsesdirektivet finder ikke anvendelse på aktiviteter, der falder uden for EU-retten. Det fremgår af artikel 4, stk. 2, i Traktaten om Den Europæiske Union, at spørgsmålet om den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar, hvilket også er nævnt i direktivets præambelbetragtning nr. 14.

Det foreslås på den baggrund, at loven – som det er tilfældet for persondataloven – ikke skal finde anvendelse på den behandling af personoplysninger, der foretages for og af politiets og forsvarets efterretningstjenester, idet denne behandling sker med henblik på varetagelsen af den nationale sikkerhed.

2.1.3.7. Retshåndhævelsesdirektivet indeholder en adgang for medlemsstaterne til at fastsætte højere standarder for beskyttelse af den registreredes rettigheder.

Det foreslås på den baggrund, at det fastsættes i loven, at regler i anden lovgivning, som giver den registrerede en bedre retstilling, går forud for reglerne i lovforslaget. Der sker dermed en videreførelse af den tilsvarende bestemmelse i persondataloven.

Der henvises i øvrigt til lovforslagets §§ 1 og 2 og bemærkningerne hertil.

2.2. Definitioner

2.2.1. Gældende ret

Databeskyttelsesdirektivet indeholder definitioner af begreberne personoplysninger, behandling, register, den registeransvarlige, registerfører, tredjemand, modtager og samtykke. Disse definitioner findes tillige i persondatalovens kapitel 2 (§ 3), idet begreberne den registeransvarlige og registerfører dog er erstattet af begreberne den dataansvarlige og databehandleren, ligesom der er tilføjet en definition på begrebet tredjeland.

2.2.2. Retshåndhævelsesdirektivet

Direktivets artikel 3 indeholder definitioner på begreberne personoplysninger, behandling, begrænsning af behandling, profilering, pseudonymisering, register, kompetent myndighed, dataansvarlig, databehandler, modtager, brud på datasikkerheden, genetiske data, biometriske data, helbredsoplysninger, tilsynsmyndighed og international organisation.

2.2.3. Justitsministeriets overvejelser og lovforslagets udformning

Justitsministeriet finder, at hensynet til at sikre, at der ikke kan opstå tvivl om implementeringen af retshåndhævelsesdirektivets artikel 3 taler for, at hovedparten af direktivets definitioner indføjes i lovforslaget, og at dette sker ved, at ordlyden af definitionerne i loven knyttes relativt tæt op ad direktivteksten.

For at øge overskueligheden foreslås det imidlertid, at enkelte af definitionerne gøres kortere og mere præcise end, hvad der følger af direktivet. Af tilsvarende årsag foreslås definitionen på begrebet pseudonymisering ikke medtaget i lovforslaget, idet dette begreb alene indgår i direktivet som et eksempel på en af de tekniske og organisatoriske foranstaltninger, som skal iværksættes efter direktivets artikel 20, jf. nærmere herom i pkt. 2.6 nedenfor.

I forlængelse af det ovenfor i pkt. 2.1 nævnte om det foreslåede anvendelsesområde for loven foreslås det endvidere, at det i definitionen af begrebet kompetente myndigheder eksplicit angives, at de kompetente myndigheder i Danmark er politiet, militærpolitiet, anklagemyndigheden, herunder den militære anklagemyndighed, kriminalforsorgen, Den Uafhængige Politiklagemyndighed og domstolene.

Der henvises i øvrigt til lovforslagets § 3 og bemærkningerne hertil.

2.3. Behandlingsregler

2.3.1. Gældende ret

Persondatalovens afsnit II indeholder en række behandlingsregler, som er relevante i politi- og straffesager i form af regler om formålet med behandlingen (§ 5), behandlingsgrundlaget for henholdsvis almindelige og følsomme personoplysninger (§§ 6-8), behandling af oplysninger i retsinformationssystemer af væsentlig samfundsmæssig betydning (§ 9), behandling af personnumre (§ 11). Hertil kommer lovens § 39 om afgørelser, der alene er truffet på baggrund af elektronisk databehandling.

2.3.1.1. Det fremgår således af persondatalovens § 5, stk. 1, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik.

God databehandlingsskik er en retlig standard, som udfyldes af tilsynsmyndighederne. Begrebet indebærer bl.a., at behandlingen af oplysninger skal være rimelig og lovlig.

Standarden anses efter praksis fra Datatilsynet for bl.a. at omfatte krav til den dataansvarlige om forudgående underretning af den registrerede om visse behandlingsaktiviteter, en pligt til at notere den registreredes indsigelser i forhold til rigtigheden af de registrerede oplysninger og underretning af berørte personer ved brud på datasikkerheden. God databehandlingsskik supplerer således navnlig lovens regler om den registreredes rettigheder.

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

Det fremgår desuden af bestemmelsens stk. 3, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Det fremgår herudover af bestemmelsens stk. 4, at behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Oplys-

ninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

Persondatalovens § 5, stk. 4, suppleres for så vidt angår grænseoverskridende udveksling af oplysninger af rammeafgørelsesbekendtgørelsens § 9, stk. 1 og 2. Det fremgår heraf, at den dataansvarlige skal træffe alle rimelige foranstaltninger til at sikre, at personoplysninger ikke videregives eller stilles til rådighed, hvis de er urigtige, ufuldstændige eller ikke ajourførte. I dette øjemed verificerer den dataansvarlige så vidt muligt kvaliteten af personoplysningerne, før de videregives eller stilles til rådighed. I forbindelse med al videregivelse af oplysninger skal der så vidt muligt tilføjes tilgængelige oplysninger, der gør det muligt for den udenlandske myndighed at vurdere, om oplysningerne er rigtige, fuldstændige, ajourførte og pålidelige.

Hvis det konstateres, at der er videregivet urigtige personoplysninger, eller at oplysningerne er videregivet ulovligt, meddeles dette straks den udenlandske myndighed. Oplysningerne skal berigtiges, slettes eller blokeres omgående, jf. bekendtgørelsens § 9, stk. 2.

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

Persondatalovens § 5, stk. 5, suppleres for så vidt angår grænseoverskridende udveksling af oplysninger af rammeafgørelsesbekendtgørelsens § 8. Det fremgår heraf, at den dataansvarlige skal tilrettelægge behandlingen af personoplysninger således, at der fastsættes passende frister for sletningen af personoplysninger eller regelmæssig undersøgelse af behovet for lagringen af oplysningerne. Det sikres endvidere ved proceduremæssige foranstaltninger, at tidsfristerne overholdes.

2.3.1.2. Persondatalovens § 6, stk. 1, indeholder en række sideordnede grundlag for behandling af almindelige personoplysninger.

Det er ikke alle behandlingsgrundlagene i bestemmelsen, der er relevante for de kompetente myndigheders behandling af personoplysninger med henblik på varetagelse af myndighedsopgaver. Disse myndigheder foretager således i dag behandling af personoplysninger, når den registrerede har meddelt samtykke hertil (stk. 1, nr. 1), når behandlingen er nødvendig for

at overholde en retlig forpligtelse, som påhviler den dataansvarlige (stk. 1, nr. 3), når behandlingen er nødvendig for at beskytte den registreredes vitale interesser (stk. 1, nr. 4), når behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse (stk. 1, nr. 5), når behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige er pålagt (stk. 1, nr. 6), eller når behandling 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 (stk. 1, nr. 7).

Det fremgår af persondatalovens § 38, at den registrerede kan tilbagekalde et samtykke.

Behandlingsgrundlagene er overlappende, og myndighedernes behandling af personoplysninger vil således ofte ske på flere af de ovennævnte behandlingsgrundlag.

2.3.1.3. Persondatalovens § 7 indeholder regler om behandling af følsomme personoplysninger. Det fremgår af bestemmelsens stk. 1, at der som hovedregel ikke må behandles oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

Bestemmelsens stk. 2-7 indeholder en række undtagelser til hovedreglen i stk.1. Det fremgår således af bestemmelsens stk. 6, at behandling af de følsomme oplysninger, der er nævnt i stk. 1, kan ske, hvis behandlingen er nødvendig af hensyn til en offentlig myndigheds varetagelse af sine opgaver på det strafferetlige område.

Lovens § 7, stk. 6, giver offentlige myndigheder adgang til at behandle følsomme personoplysninger i straffesager. Bestemmelsen giver således f.eks. politi og anklagemyndighed mulighed for at registrere oplysninger om f.eks. race og hudfarve i forbindelse med efterforskningsvirksomhed, idet disse oplysninger kan være nødvendige identifikationsoplysninger.

Persondatalovens § 7, stk. 6, suppleres for så vidt angår grænseoverskridende udveksling af oplysninger af rammeafgørelsesbekendtgørelsens § 2, stk. 2. Det fremgår heraf, at behandling af oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fag-

foreningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold efter persondatalovens § 7, stk. 6, ikke må ske, medmindre behandlingen er strengt nødvendig.

Persondatalovens § 8 indeholder særregler om den offentlige forvaltnings behandling af andre kategorier af følsomme oplysninger end dem, der er nævnt i § 7, stk. 1. Det fremgår af bestemmelsens stk. 1, at der ikke for den offentlige forvaltning 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 fremgår videre af bestemmelsens stk. 2, at der ikke må ske videregivelse af sådanne oplysninger, med mindre en af betingelserne i stk. 2, nr. 1-4, er opfyldt.

Det fremgår imidlertid af bestemmelsens stk. 6, at behandling og videregivelse efter stk. 1 og 2 kan finde sted, hvis betingelserne i lovens § 7 er opfyldt. De kompetente myndigheder vil således også have mulighed for at behandle oplysninger omfattet af § 8 i straffesager, jf. lovens § 7, stk. 6.

Rammeafgørelsesbekendtgørelsens §§ 3 og 5 indeholder særlige regler om adgangen til at behandle oplysninger, der er modtaget fra eller stillet til rådighed af en udenlandsk myndighed.

Det fremgår således af bekendtgørelsens § 3, at sådanne oplysninger kun må behandles til en række nærmere angivne andre formål end dem, hvortil de blev videregivet eller stillet til rådighed. Oplysningerne kan anvendes med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner i forbindelse med andre straffelovsovertrædelser eller sanktioner end dem, hvortil de blev videregivet eller stillet til rådighed, eller andre retlige og administrative procedurer, som hænger direkte sammen med disse formål. Behandling kan endvidere ske med henblik på afværgelse af en umiddelbar og alvorlig trussel mod den offentlige sikkerhed, eller ethvert andet formål med forhåndsgodkendelse fra den videregivende myndighed eller med den registreredes samtykke.

Behandling må endvidere ske i historisk, statistisk eller videnskabeligt øjemed, såfremt oplysningerne gøres anonyme.

Behandlingen må ikke ske i strid med specifikke begrænsninger for behandling af videregivne oplysninger fastsat i lovgivningen gældende for den videregivende udenlandske myndighed, når den videregivende myndighed gør opmærksom på begrænsningerne.

Det fremgår videre af bekendtgørelsens § 5, at personoplysninger, som er modtaget fra eller stillet til rådighed af en udenlandsk myndighed, kun må videregives til private, hvis den videregivende udenlandske myndighed har givet tilladelse til videregivelse i henhold til sin nationale lovgivning og den registreredes specifikke legitime interesser ikke forhindrer videregivelse. Det er endvidere at krav, at videregivelse af oplysninger i særlige tilfælde er afgørende for den dataansvarlige, der videregiver oplysningerne til en privat, af hensyn til udførelsen af en opgave, den er blevet pålagt ved lov, forebyggelse, efterforskning, afsløring eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner, afværgelse af en umiddelbar og alvorlig trussel mod den offentlige sikkerhed, eller forebyggelse af alvorlige krænkelser af enkeltpersoners rettigheder.

Den dataansvarlige, der videregiver oplysningerne til en privatperson, orienterer denne om, hvilke formål oplysningerne udelukkende må anvendes til.

2.3.1.4. Persondataloven indeholder ikke generelle regler om tidsfrister for sletning af personoplysninger.

Som nævnt ovenfor i pkt. 2.3.1.1 fremgår det imidlertid af persondatalovens § 5, stk. 5, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Reglen suppleres af rammeafgørelsesbekendtgørelsens § 8.

Bestemmelsen indebærer, at den dataansvarlige skal vurdere, hvor længe oplysningerne skal opbevares, hvilket ofte vil ske gennem generelle slettefrister.

Persondatalovens § 5, stk. 5, er berørt i forarbejderne til lov nr. 1727 af 27. december 2016 om ændring af lov om Politiets Efterretningstjeneste (PET), jf. Folketingstidende 2016-17, A, L 71 som fremsat den 9. november 2016.

Det fremgår af lovforslagets pkt. 3.1.2.4.1, at i de situationer, hvor der er fastsat generelle slettefrister, er det Justitsministeriets opfattelse, at der ikke af bestemmelsen i persondatalovens § 5, stk. 5, kan udledes en pligt for en dataansvarlig myndighed til løbende at gennemgå samtlige sine sager, dokumenter mv. med henblik på at sikre, at der ikke opbevares konkrete personoplysninger i strid med persondatalovens § 5, stk. 5, så længe myndigheden har procedurer, som sikrer, at der sker sletning i overensstemmelse med de fastsatte frister.

For så vidt angår personoplysninger i Det Centrale Kriminalregister er der med hjemmel i persondatalovens § 32, stk. 5, og § 72 fastsat nærmere regler om bl.a. sletttefristen, jf. bekendtgørelse nr. 881 af 4. juli 2014 om behandling af personoplysninger i Det Centrale Kriminalregister (Kriminalregisteret) som senest ændret ved bekendtgørelse nr. 99 af 26. januar 2017.

2.3.1.5. Persondatalovens § 9 indeholder regler om personoplysninger, som behandles i retsinformationssystemer. Det fremgår således af bestemmelsens stk. 1, at behandling af følsomme oplysninger og oplysninger om rent private forhold kan ske med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for førelsen af systemerne.

2.3.1.6. Persondatalovens § 11 indeholder regler om behandlingen af oplysninger om personnummer. Det fremgår af bestemmelsens stk. 1, at offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer.

2.3.1.7. Persondatalovens § 39 indeholder regler om afgørelser, der alene er truffet på baggrund af elektronisk databehandling. Efter bestemmelsens stk. 1 kan der som hovedregel ikke træffes en sådan automatisk afgørelse, der har retsvirkninger for eller i øvrigt berører den pågældende i væsentlig grad, hvis den registrerede gør indsigelse herimod.

Bestemmelsens stk. 2 indeholder undtagelser til hovedreglen i stk. 1, herunder en mulighed for at træffe sådanne afgørelser, hvis det er hjemlet i en lov, der indeholder bestemmelser til beskyttelse af den registreredes berettigede interesser.

Bestemmelsens stk. 3 indeholder en ret for den registrerede til at blive gjort bekendt med, hvilke beslutningsregler der ligger bag en sådan automatisk afgørelse.

Bestemmelsen i § 39 finder ikke anvendelse for politiets, anklagemyndighedens og domstolenes behandling af personoplysninger inden for det strafferetlige område, jf. persondatalovens § 2, stk. 4. Bestemmelsen er således alene relevant i forhold til de øvrige kompetente myndigheders behandling af personoplysninger.

2.3.2. Retshåndhævelsesdirektivet

Retshåndhævelsesdirektivets kapitel II indeholder regler om principper for behandling af personoplysninger. Kapitlet indeholder regler om de generelle principper for behandling af personoplysninger (artikel 4), tidsfrister for opbevaring og revision (artikel 5), krav om sondring mellem forskellige kategorier af registrerede og personoplysninger samt kontrol med kvaliteten af personoplysninger (artiklerne 6 og 7), betingelserne for lovlig behandling (artiklerne 8-10) og om automatiske individuelle afgørelser (artikel 11).

2.3.2.1. Det fremgår af direktivets artikel 4, at personoplysninger skal behandles lovligt og rimeligt (litra a), indsamles til udtrykkeligt angivne og legitime formål og ikke behandles på en måde, der er uforenelig med disse formål (litra b), være tilstrækkelige, relevante og ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de behandles (litra c), 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 (litra d), 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 behandles (litra e), og behandles på en måde, der sikrer en 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 (litra f).

Det fremgår videre af bestemmelsens stk. 2, at behandling, der foretages af den samme eller en anden dataansvarlig til et andet formål omfattet af artikel 1, stk. 1, end det, hvortil personoplysningerne er indsamlet, er tilladt i det omfang, at den dataansvarlige er bemyndiget til at behandle sådanne personoplysninger til et sådant formål i overensstemmelse med EU-retten eller medlemsstaternes nationale ret, og at behandlingen er nødvendig for

og forholdsmæssig i forhold til dette andet formål i overensstemmelse med EU-retten eller medlemsstaternes nationale ret.

Behandling, der foretages af den samme eller en anden dataansvarlig, kan omfatte behandling til arkivformål i samfundets interesse eller til videnskabelig, statistisk eller historisk brug med henblik på direktivets formål, forudsat at behandlingen er omfattet af de fornødne garantier for den registreredes rettigheder og frihedsrettigheder, jf. artikel 4, stk. 3.

Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1, 2 og 3 overholdes, jf. artikel 4, stk. 4.

2.3.2.2. Det fremgår af direktivets artikel 5, at der skal fastsættes hensigtsmæssige tidsfrister for sletning af personoplysninger eller for regelmæssig revision af behovet for opbevaring af personoplysninger. Det sikres ved proceduremæssige foranstaltninger, at disse tidsfrister overholdes.

2.3.2.3. Direktivets artikel 6 og artikel 7, stk. 1, indeholder krav om, at der skal sondres mellem henholdsvis forskellige kategorier af registrerede og personoplysninger.

Den dataansvarlige skal, hvor det er relevant og så vidt muligt, klart sondre mellem personoplysninger om forskellige kategorier af registrerede. Der skal f.eks. sondres mellem personer, om hvem der er væsentlig grund til at tro, at de har begået eller vil begå en strafbar handling og ofre for en strafbar handling, jf. artikel 6.

Det fremgår af direktivets præambelbetragtning nr. 31, at behandling af personoplysninger inden for retligt samarbejde i straffesager og politisamarbejde i sagens natur indebærer behandling af personoplysninger om forskellige kategorier af registrerede. Der bør således, hvis det er relevant og så vidt muligt, sondres klart mellem personoplysninger om forskellige kategorier af registrerede såsom mistænkte, personer, der er dømt for en strafbar handling, ofre og andre parter som f.eks. vidner, personer, der ligger inde med relevante oplysninger eller kontakter, eller mistænktes og dømte kriminelles ledsagepersoner. Dette bør ikke være til hinder for anvendelsen af princippet om uskyldsformodning, som er sikret ved chartret og ved EMRK, som fortolket i retspraksis ved henholdsvis Domstolen og Den Europæiske Menneskerettighedsdomstol.

Den dataansvarlige skal endvidere så vidt muligt sondre mellem personoplysninger, der bygger på faktiske omstændigheder, og personoplysninger, der bygger på personlige vurderinger, jf. artikel 7.

Det fremgår af direktivets præambelbetragtning nr. 30, at princippet om oplysningernes rigtighed bør anvendes under hensyntagen til den pågældende behandlings karakter og formål. Navnlig i retssager er udsagn, der indeholder personoplysninger, baseret på en subjektiv opfattelse af fysiske personer, og det er ikke altid muligt at kontrollere dem. Kravet om oplysningernes rigtighed bør derfor ikke vedrøre et udsagns rigtighed, men blot det forhold, at der er fremsat et konkret udsagn.

2.3.2.4. Direktivets artikel 7, stk. 2 og 3, indeholder regler om de dataansvarliges pligt til at sikre, at oplysninger, der videregives, er rigtige, fuldstændige og pålidelige.

De kompetente myndigheder skal således iværksætte alle rimelige tiltag for at sikre, at personoplysninger, som er urigtige, ufuldstændige eller ikke ajourførte, ikke videregives eller stilles til rådighed. Med henblik herpå kontrollerer hver kompetent myndighed, så vidt det er praktisk muligt, kvaliteten af personoplysninger, før disse videregives eller stilles til rådighed. I forbindelse med al videregivelse af personoplysninger skal nødvendige oplysninger, der gør det muligt for den modtagende kompetente myndighed at vurdere, i hvor høj grad personoplysningerne er rigtige, fuldstændige og pålidelige, og i hvilket omfang de er ajourførte, så vidt muligt tilføjes.

Hvis det konstateres, at der er videregivet urigtige personoplysninger, eller at personoplysninger er videregivet ulovligt, skal dette straks meddeles modtageren. I så fald skal personoplysningerne berigtiges eller slettes, eller behandling skal begrænses i overensstemmelse med direktivets artikel 16.

2.3.2.5. Direktivets artikel 8 og 10 indeholder henholdsvis betingelser for behandling af almindelige oplysninger og særlige kategorier af oplysninger.

Det fremgår således af direktivets artikel 8, at behandling kun er lovlig, hvis og i det omfang denne behandling er nødvendig for, at en kompetent myndighed kan udføre en opgave med henblik på direktivets formål, og hvis behandlingen sker på grundlag af EU-retten eller national ret.

Efter artikel 10 er 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 kun tilladt, når det er strengt nødvendigt, forudsat at behandlingen er omfattet af de fornødne garantier for den registreredes rettigheder og frihedsrettigheder, og kun hvis behandlingen er hjemlet i EU-retten eller national ret, hvis behandlingen sker for at beskytte den registreredes eller en anden fysisk persons vitale interesser, eller hvis behandlingen vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede.

Det fremgår af direktivets præambelbetragtning nr. 35, at udførelsen af opgaverne med at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger, som institutionelt er tillagt de kompetente myndigheder ved lov, gør det muligt for disse myndigheder at kræve, at fysiske personer efterlever de anmodninger, der fremsættes. I så fald bør den registreredes samtykke som defineret i databeskyttelsesforordningen ikke udgøre et retsgrundlag for de kompetente myndigheders behandling af personoplysninger. Hvis det kræves, at den registrerede opfylder en retlig forpligtelse, har den registrerede ikke et reelt og frit valg, hvorfor den registreredes reaktion ikke kan anses for at være en frivillig viljetilkendegivelse. Dette bør ikke forhindre medlemsstaterne i ved lov at fastsætte bestemmelser om, at den registrerede kan acceptere behandling af vedkommendes personoplysninger med henblik på dette direktiv, som f.eks. DNA-test i strafferetlige efterforskninger eller elektronisk overvågning af vedkommendes geografiske position ved elektronisk fodlænke med henblik på fuldbyrdelse af strafferetlige sanktioner.

2.3.2.6. Direktivets artikel 9 indeholder en regel om særlige betingelser for behandling.

Personoplysninger, der er indsamlet med henblik på et af direktivets formål, må alene anvendes til andre formål, hvis der er hjemmel hertil i EU-retten eller national ret, jf. stk. 1.

Efter bestemmelsens stk. 3 skal den videregivende kompetente myndighed, hvis EU-retten eller national ret fastsætter særlige vilkår for behandling, underrette modtageren af sådanne personoplysninger om disse vilkår og

kravet om at overholde dem. De kompetente myndigheder må ikke stille andre vilkår for andre medlemsstater eller EU-agenturer mv. end for andre nationale myndigheder, jf. stk. 4.

Det fremgår af direktivets præambelbetragtning nr. 36, at når EU-retten eller medlemsstatens nationale ret, der finder anvendelse for den videregivende kompetente myndighed, fastsætter særlige vilkår, der finder anvendelse under særlige omstændigheder på behandling af personoplysninger, såsom anvendelse af regler for behandling af oplysninger, skal den videregivende kompetente myndighed underrette modtageren af sådanne personoplysninger om disse vilkår og kravet om at opfylde dem. Sådanne vilkår kunne f.eks. indebære et forbud mod at videregive personoplysninger til andre, eller at anvende dem til andre formål end dem, på baggrund af hvilke de blev videregivet til modtageren, eller at underrette den registrerede i tilfælde af en begrænsning af retten til oplysninger uden forudgående godkendelse fra den videregivende kompetente myndighed. Disse forpligtelser bør også finde anvendelse for overførsler fra den videregivende kompetente myndighed til modtagere i tredjelande eller internationale organisationer.

2.3.2.5. Direktivets artikel 11 indeholder regler om automatiske individuelle afgørelser.

En afgørelse, der alene er baseret på automatisk behandling, herunder profilering, som har negativ retsvirkning for den registrerede eller betydeligt påvirker den pågældende, er forbudt, medmindre den er hjemlet i EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt, og som fastsætter de fornødne garantier for den registreredes rettigheder og frihedsrettigheder, i det mindste den registreredes ret til menneskelig indgriben fra den dataansvarliges side.

Efter bestemmelsens stk. 2 må sådanne afgørelser ikke baseres på særlige kategorier af personoplysninger, jf. pkt. 2.3.2.5, medmindre der er indført passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser.

Profilering, der fører til forskelsbehandling af fysiske personer på grundlag af særlige kategorier af personoplysninger, jf. artikel 10, er forbudt i henhold til EU-retten, jf. stk. 3.

2.3.3. Justitsministeriets overvejelser og lovforslagets udformning

2.3.3.1. Direktivets artikel 4 indeholder de generelle principper for behandling af personoplysninger. Principperne svarer i vidt omfang til de principper, som er indeholdt i persondatalovens § 5, stk. 1-5. Disse principper finder allerede i dag anvendelse i forhold til de kompetente myndigheder.

Det krav, som findes i direktivets artikel 4, stk. 1, litra f, fremgår ikke af persondatalovens § 5. Det fremgår af artikel 4, stk. 1, litra f, at personoplysninger skal behandles på en måde, der sikrer en 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. Der er således tale om en henvisning til de tekniske og organisatoriske foranstaltninger, som skal fastsættes for at overholde kravene i forhold til behandlingssikkerhed. Der findes en næsten tilsvarende regel i persondatalovens § 41, stk. 3.

Det foreslås på den baggrund, at der i overensstemmelse med retshåndhævelsesdirektivets artikel 4 fastsættes de generelle principper for behandling af personoplysninger.

Det bemærkes i den forbindelse, at det foreslås, at kravet i direktivets artikel 4, stk. 1, litra a, om, at behandlingen skal være lovlig og rimelig, implementeres på samme måde som persondatalovens implementering af den tilsvarende bestemmelse i databeskyttelsesdirektivet. Det foreslås således i lovforslagets § 4, stk. 1, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik. Dette indebærer, at der – på samme måde som i dag – vil være tale om en retlig standard, som skal udfyldes af tilsynsmyndighederne. Der videreføres herved en ordning, som er velkendt for såvel tilsynsmyndighederne som for de omfattede kompetente myndigheder.

Direktivets artikel 4, stk. 2, indeholder regler om adgangen for den samme eller en anden dataansvarlig til at behandle oplysninger til et andet formål omfattet af direktivet.

Der er tale om en væsentlig bestemmelse, som gør det muligt for de kompetente myndigheder at behandle oplysninger til flere forskellige formål. Det er f.eks. relevant i forhold til den videregivelse af personoplysninger, som finder sted i forbindelse med en straffesags forløb. Politiet kan således

indsamle oplysninger om en mistænkts telefonnummer i forbindelse med efterforskningen af et strafbart forhold. Hvis der indledes en straffesag, vil oplysningen om den (nu) tiltaltes telefonnummer blive videregivet til domstolene til brug for forkyndelse af anklageskrift og indkaldelse til hovedforhandling. Hvis den pågældende findes skyldig og idømmes en fængselsstraf, vil oplysningerne om den (nu) dømtes telefonnummer blive videregivet til kriminalforsorgen til brug for besked om indkaldelse til afsoning.

Det foreslås på den baggrund, at der fastsættes regler om, at senere behandling til et andet formål omfattet af loven, kan ske på baggrund af lov, og hvis det er nødvendigt og forholdsmæssigt i forhold til dette efterfølgende formål. Begrebet "lov" vil i denne forbindelse omfatte enhver eksisterende regulering, der generelt eller konkret hjemler, at behandling kan finde sted. Dette vil således også omfatte nærværende lov i det omfang en konkret behandling til et andet formål kan anses for at være hjemlet herved.

Der henvises i øvrigt til lovforslagets §§ 4 og 5 og bemærkningerne hertil.

2.3.3.2. Direktivets artikel 5 indeholder krav om tidsfrister for sletning og revision.

Som nævnt ovenfor i pkt. 2.3.1.4 indeholder persondataloven i dag en generel regel om, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Direktivets krav om, at den dataansvarlige skal fastsætte tidsfrister for sletning, udgør efter Justitsministeriets opfattelse i vidt omfang en videreførelse af gældende ret.

Det foreslås på den baggrund, at der i overensstemmelse med retshåndhævelsesdirektivets artikel 5 fastsættes en regel om, at den dataansvarlige myndighed skal fastsætte tidsfrister for, hvornår de indsamlede oplysninger skal slettes. Det sikres herved, at der ikke opstår tvivl om, at der er sket en korrekt implementering af direktivet.

Der henvises i øvrigt til lovforslagets § 7 og bemærkningerne hertil.

2.3.3.3. Direktivets artikel 6 og artikel 7, stk. 1, indeholder krav om, at der skal sondres mellem henholdsvis forskellige kategorier af registrerede og personoplysninger.

Kravene har efter Justitsministeriets opfattelse til formål at sikre, at den dataansvarlige anvender en differentieret tilgang til, om behandlingskravene er opfyldt. En sådan sondring kan således f.eks. være relevant, når den dataansvarlige skal vurdere, om de indsamlede oplysninger kan anses for at være korrekte, eller hvornår oplysningerne skal slettes.

Persondataloven indeholder ikke eksplicitte regler om, at de kompetente myndigheder skal foretage sådanne sondringer. Overholdelsen af de almindelige databehandlingsprincipper vil imidlertid efter Justitsministeriets opfattelse medføre, at der allerede i dag er behov for, at de kompetente myndigheder, inden en konkret behandling iværksættes, inddrager spørgsmålet om, hvilken kategori af registreret person der er tale om.

Hertil kommer, at også praksis fra Den Europæiske Menneskerettighedsdomstol forudsætter, at der i visse sammenhænge skal sondres mellem forskellige kategorier af registrerede, jf. Domstolens dom af 4. december 2008 (i sagen S og Marper mod Det Forenede Kongerige, sagsnr. 30562). Domstolene tog i sagen stilling til en ordning i Det Forenede Kongerige, hvorefter oplysninger fra mistænkte om fingeraftryk, celleprøver og DNA blev opbevaret uden tidsbegrænsning og uden hensyntagen til, om de pågældende efterfølgende blev dømt for et strafbart forhold. Domstolen fandt, at denne ordning var i strid med Den Europæiske Menneskerettighedskonventions artikel 8 om retten til privatliv, idet Domstolen bl.a. henviste til, at den omstændighed, at mistænktes og dømtes DNA-oplysninger blev opbevaret på samme måde ikke var i overensstemmelse med princippet om uskyldsformodningen.

Det foreslås på den baggrund, at der i overensstemmelse med retshåndhævelsesdirektivets artikel 6 fastsættes en regel om, at den dataansvarlige skal sondre mellem forskellige typer af registrerede. Det sikres herved, at der ikke opstår tvivl om, at der er sket en korrekt implementering af direktivet.

Det foreslås endvidere, at der i forbindelse med den generelle regel om behandlingsprincipperne fastsættes et krav om, at den dataansvarlige skal tage hensyn til oplysningernes karakter ved behandlingen.

Der henvises i øvrigt til lovforslagets § 4, stk. 1, og § 8 og bemærkningerne hertil.

2.3.3.4. Direktivets artikel 7, stk. 2, indeholder regler om de dataansvarliges pligt til at sikre, at oplysninger, der videregives, er rigtige, fuldstændige og pålidelige, samt et krav om at der ved videregivelsen så vidt mulig tilføjes nødvendige oplysninger, der gør det muligt for den modtagende kompetente myndighed at vurdere, i hvor høj grad personoplysningerne er rigtige, fuldstændige og pålidelige, og i hvilket omfang de er ajourførte. Bestemmelsens stk. 3 indeholder et krav om, at en modtager skal underrettes, hvis der er sket videregivelse af urigtige oplysninger, eller at oplysninger er videregivet ulovligt, hvorefter der skal ske berigtigelse, sletning eller begrænsning.

Direktivet svarer på dette punkt til rammeafgørelsesbekendtgørelsens § 9, stk. 1 og 2.

Det foreslås på den baggrund, at der i overensstemmelse med retshåndhævelsesdirektivets artikel 7, stk. 2, fastsættes en regel om den dataansvarliges forpligtelser i forbindelse med videregivelse. Der er som nævnt ovenfor tale om en udvidelse af den forpligtelse, som allerede i dag gælder efter rammeafgørelsesbekendtgørelsen.

Der henvises i øvrigt til lovforslagets § 4, stk. 5, og bemærkningerne hertil.

2.3.3.5. Direktivets artikel 8 indeholder et krav om, at medlemsstaterne skal fastsætte bestemmelser om, at behandling kun er lovlig, hvis og i det omfang denne behandling er nødvendig for, at en kompetent myndighed kan udføre en opgave med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed, og at den sker på grundlag af EU-retten eller medlemsstaternes nationale ret.

Det foreslås på den baggrund, at der i overensstemmelse med direktivets artikel 8 fastsættes en regel om, at behandling af oplysninger kun må finde sted, når behandlingen er nødvendig for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

Den foreslåede bestemmelse erstatter således de behandlingsgrundlag efter persondataloven, som de kompetente myndigheder i dag anvender til behandling af personoplysninger, herunder behandling af personnumre med henblik på de formål, som er nævnt i § 1, stk. 1.

Justitsministeriet finder således ikke, at der er behov for, at der i nærværende lov indsættes en særlig adgang for de kompetente myndigheder til at behandle oplysninger om personnummer svarende til persondatalovens § 11.

Hvis de kompetente myndigheder behandler oplysninger om personnummer til et formål, som falder uden for det foreslåede anvendelsesområde for nærværende lov, vil behandlingen fortsat skulle ske i medfør af persondatalovens § 11.

De kompetente myndigheder vil – uanset om behandlingen sker i medfør af nærværende lov eller persondataloven – også fremover skulle overholde reglerne i CPR-loven, jf. lovbekendtgørelse nr. 5 af 9. januar 2013 om Det Centrale Personregister med senere ændringer.

Justitsministeriet finder desuden ikke, at der er grundlag for, at de kompetente myndigheder skal behandle oplysninger på grundlag af et samtykke fra den registrerede, jf. herved henvisningen til direktivets præambelbetragtning nr. 35 i pkt. 2.4.3.5 ovenfor. Et eventuelt samtykke fra den registrerede vil imidlertid kunne indgå i den dataansvarlige myndigheds vurdering af, om en given behandling kan anses for at være nødvendig.

Det bemærkes endvidere, at behandlingen af personoplysninger med henblik på førelse af retsinformationssystemer – som i dag sker efter persondatalovens § 9 – ikke varetager et formål, der er omfattet af det foreslåede anvendelsesområde. Behandling af personoplysninger til dette formål vil i stedet fortsat skulle ske efter persondatalovens § 9 og – fra den 25. maj 2018 – databeskyttelsesforordningen.

Der henvises i øvrigt til lovforslagets § 9 og bemærkningerne hertil.

2.3.3.6. Direktivets artikel 10 indeholder krav vedrørende behandling af særlige kategorier af personoplysninger. Der er tale 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.

De i bestemmelsen oplistede særlige kategorier svarer i vidt omfang til de særlige kategorier af oplysninger, som er omfattet af databeskyttelsesdirektivets artikel 8, som er implementeret i persondatalovens § 7. Retshåndhævelsesdirektivets artikel 10 tilføjer således alene genetiske data samt biometriske data med det formål entydigt at identificere en fysisk person.

I overensstemmelse med de gældende regler for offentlige myndigheders behandling af følsomme oplysninger i straffesager, jf. pkt. 2.3.1.3 ovenfor, foreslås der i lovforslagets § 10 fastsat en regel om, at de kompetente myndigheder under overholdelse af betingelserne i loven kan foretage behandling af oplysninger omfattet af stk. 1, når det er strengt nødvendigt med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

Der er i forhold til behandlingsgrundlaget for almindelige personoplysninger i den foreslåede § 9 således tale om et skærpet krav til nødvendigheden, idet behandlingen for så vidt angår disse særlige kategorier af oplysninger skal være strengt nødvendig. Kravet er desuden skærpet i forhold til den gældende bestemmelse i persondatalovens § 7, stk. 6.

I praksis vil det dog formentlig ikke være muligt at angive nogen væsentlig forskel på kriterierne ”nødvendigt” og ”strengt nødvendigt”. Det gælder således bl.a. i relation til politiets mv. adgang til at behandle de nævnte typer af følsomme personoplysninger med henblik på kriminalitetsbekæmpelse, f.eks. behandling af oplysninger om politisk overbevisning i forbindelse med opklaring af et politisk motiveret mord, eller behandling af oplysninger om race med henblik på at identificere en gerningsmand.

Persondatalovens § 8 indeholder som nævnt oven for i pkt. 2.3.1.3 et særligt grundlag for behandling af oplysninger om rent private forhold. Der er efter Justitsministeriets opfattelse ikke behov for at videreføre dette behandlingsgrundlag. Sådanne oplysninger vil således kunne ske efter det almindelige behandlingsgrundlag, jf. pkt. 2.3.3.5 ovenfor.

Der henvises i øvrigt til lovforslagets § 10 og bemærkningerne hertil.

2.3.3.7. Direktivets artikel 11 indeholder en bestemmelse om adgangen til at træffe afgørelser alene på grundlag af automatisk behandling, herunder profilering.

Persondatalovens § 39 indeholder en bestemmelse om afgørelser, der alene er truffet på baggrund af elektronisk databehandling. Bestemmelsen finder imidlertid ikke anvendelse på politiets, anklagemyndighedens og domstolenes behandling af personoplysninger inden for det strafferetlige område.

De myndigheder, som er omfattet af lovforslagets anvendelsesområde, træffer ikke i dag afgørelser alene på grundlag af automatisk behandling.

Det bemærkes i den forbindelse, at der ved lov nr. 372 af 14. april 2014 om ændring af færdselsloven (Indførelse af betinget objektivt ansvar for ejer (bruger) af et motorkøretøj for visse hastighedsovertrædelser) blev indført en bestemmelse i færdselslovens § 118 c, hvorefter ejeren (brugeren) af køretøjet blev pålagt et objektivt bødeansvar for hastighedsoverskridelser, der var konstateret ved automatisk trafikkontrol (ATK).

Det fremgår af lovforslaget (Folketingstidende 2013-14, A, L 74 som fremsat den 14. november 2013), pkt. 4.1.3, at der ved en hastighedsmåling, der er foretaget med ATK, sker en manuel vurdering af de enkelte billeder i forhold til, om måling og kvalitet er tilstrækkelig til, at der kan indledes en straffesag.

Det kan imidlertid ikke udelukkes, at den teknologiske udvikling vil føre til, at der i fremtiden kan optages fotos med ATK af en sådan kvalitet, at en manuel vurdering ikke vil være nødvendig, hvorefter en afgørelse om, at der skal indledes en straffesag – i første omgang i form af et bødeforelæg – i princippet kan ske alene på baggrund af automatisk databehandling. Der kan med andre blive tale om, at bødeforelægget automatisk sendes til ejeren (brugeren) af køretøjet.

Det foreslås på den baggrund i lovforslagets § 11, at der fastsættes en bestemmelse om, at der kan træffes automatiske afgørelser, såfremt der findes passende foranstaltninger for at sikre den registreredes interesser, herunder en adgang for den registrerede til en kræve en menneskelig indgriben fra den dataansvarliges side. Det vil i ovennævnte eksempel indebære, at en ejer, der har modtaget en afgørelse om, at den pågældende ifalder bødeansvar efter en hastighedsmåling med ATK, vil kunne kræve, at poli-

tiet foretager en manuel vurdering af det eller de optagne fotos, og at politiet på den baggrund tager stilling til, om der skal indledes en straffesag.

De afgørelser, som i givet fald vil være omfattet af bestemmelsen, vil alene være myndighedsafgørelser i forvaltningslovens forstand, dvs. udtalelser, der går ud på at fastsætte, hvad der er eller skal være ret i et foreliggende tilfælde, idet automatiske afgørelser ikke vil blive truffet af domstolene.

Der henvises i øvrigt til lovforslagets § 11 og bemærkningerne hertil.

2.4. Den registreredes rettigheder

2.4.1. Gældende ret

2.4.1.1. Som nævnt ovenfor i pkt. 1.3.1 gælder persondataloven generelt for de kompetente myndigheders behandling af personoplysninger. Lovens bestemmelser om oplysningspligt over for den registrerede (kapitel 8), og den registreredes ret til indsigelse, berigtigelse, blokering og sletning af personoplysninger (§§ 35-37) finder dog ikke anvendelse på behandlinger, der foretages for domstolene, politiet og anklagemyndigheden inden for det strafferetlige område. Herudover finder lovens regler om den registreredes ret til indsigt (kapitel 9) ikke anvendelse på behandlinger, der foretages for domstolene inden for det strafferetlige område.

Som nævnt ovenfor i pkt. 1.3.2 finder persondatalovens kapitel 9 om den registreredes indsigtsret og § 37 om berigtigelse mv. anvendelse for så vidt angår de kompetente myndigheders behandling af personoplysninger, der udveksles eller stilles til rådighed mellem en dansk og en udenlandsk myndighed i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager inden for Den Europæiske Union og Schengen-samarbejdet, jf. rammeafgørelsesbekendtgørelsens § 2.

2.4.1.2. Det fremgår af persondatalovens § 28, stk. 1, at den dataansvarlige eller dennes repræsentant ved indsamling af oplysninger hos den registrerede skal give den registrerede meddelelse om den dataansvarliges og dennes repræsentants identitet, formålene med den behandling, hvortil oplysningerne er bestemt, og alle yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser. Som eksempler på sådanne yderligere oplysninger nævnes i stk. 1 kategorierne af modtagere, om det er obligatorisk eller frivilligt at besvare stillede

spørgsmål samt mulige følger af ikke at svare, og om reglerne om indsigt i og om berigtigelse af de oplysninger, der vedrører den registrerede. Bestemmelsen i stk. 1 gælder ikke, hvis den registrerede allerede er bekendt med disse oplysninger, jf. stk. 2.

Det fremgår videre af persondatalovens § 29, stk. 1, at hvor oplysninger ikke er indsamlet hos den registrerede, påhviler det den dataansvarlige eller dennes repræsentant ved registreringen, eller hvor de indsamlede oplysninger er bestemt til videregivelse til tredjemand, senest når videregivelsen af oplysningerne finder sted, at give den registrerede meddelelse om den dataansvarliges og dennes repræsentants identitet, formålene med den behandling, hvortil oplysningerne er bestemt, og alle yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser. Som eksempler på sådanne yderligere oplysninger nævnes i stk. 1 hvilken type oplysninger det drejer sig om, kategorierne af modtagere og om reglerne om indsigt i og om berigtigelse af de oplysninger, der vedrører den registrerede. Bestemmelsen i stk. 1 gælder ikke, hvis den registrerede allerede er bekendt med disse oplysninger, hvis registreringen eller videregivelsen udtrykkeligt er fastsat ved lov eller bestemmelser fastsat i henhold til lov, eller hvis underretning af den registrerede viser sig umulig eller er uforholdsmæssigt vanskelig, jf. stk. 2 og 3.

Persondatalovens § 30 indeholder regler om, hvornår der kan gøres undtagelse fra §§ 28 og 29. Det fremgår således af bestemmelsens 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.

Undtagelse fra bestemmelserne i § 28, stk. 1, og § 29, stk. 1, 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 statens sikkerhed (nr. 1), forsvaret (nr. 2), den offentlige sikkerhed (nr. 3), forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv (nr. 4), væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender (nr. 5), og kontrol-, tilsyns- eller reguleringsopgaver, herunder opgaver af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i nr. 3-5 nævnte områder (nr. 6).

2.4.1.3. Persondatalovens §§ 31-34 indeholder regler om den registreredes indsigtsret.

Det fremgår således af persondatalovens § 31, at når en person fremsætter begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om, hvilke oplysninger der behandles, behandlingens formål, kategorierne af modtagere af oplysningerne og tilgængelig information om, hvorfra disse oplysninger stammer.

Den dataansvarlige skal snarest besvare begæringer som nævnt i stk. 1. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om, hvornår afgørelsen kan forventes at foreligge, jf. stk. 2.

Persondatalovens § 32 indeholder en række undtagelser til indsigtsretten efter § 31. Det fremgår således af bestemmelsens stk. 1, at retten til indsigt ikke gælder, hvis betingelserne i § 30 er opfyldt, jf. ovenfor i pkt. 2.4.1.2.

Det fremgår videre af bestemmelsens 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.

Bestemmelsen i § 31, stk. 1, finder heller ikke 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, jf. stk. 4.

Det fremgår desuden af bestemmelsens stk. 5, at for behandling af oplysninger på det strafferetlige område, der foretages for den offentlige forvaltning, kan justitsministeren fastsætte undtagelser fra retten til at få oplysninger efter § 31, stk. 1, for så vidt bestemmelsen i § 32, stk. 1, jf. herved § 30, må antages at medføre, at begæringer om ret til indsigt i almindelighed må afslås.

Justitsministeren har anvendt bemyndigelsesbestemmelsen i lovens § 32, stk. 5, til ved bekendtgørelse at gøre undtagelse fra indsigtsretten. Det følger således af § 13 i bekendtgørelse nr. 1776 af 16. december 2015 om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG), at indsigtsretten ikke finder anvendelse i forhold til oplysninger, der behandles i ANPG-systemet. Tilsvarende følger det af § 13, stk. 1, i bekendtgørelse nr. 921 af 2. juli 2010 om behandling af personoplysninger i Politiets Efterforskningsstøtte Database (PED), at indsigtsretten som udgangspunkt ikke finder anvendelse i forhold til oplysninger behandlet i PED.

Det fremgår herudover af persondatalovens § 33, at en registreret person, der har fået meddelelse efter § 31, stk. 1, ikke har krav på ny meddelelse før 6 måneder efter sidste meddelelse, medmindre der godtgøres en særlig interesse heri.

Endeligt fremgår det af persondatalovens § 34, at meddelelser i henhold til § 31, stk. 1, på begæring skal gives skriftligt. I tilfælde, hvor hensynet til den registrerede taler derfor, kan meddelelse dog gives i form af en mundtlig underretning om indholdet af oplysningerne.

Retsplejelovens kapitel 66 indeholder regler om sigtede personers mv. adgang til materiale, som er tilvejebragt af politiet i forbindelse med strafferetlig forfølgning. Retsplejeloven indeholder endvidere regler om aktindsigt i domme, kendelser og andre dokumenter, der vedrører en straffesag. Udgangspunktet er, at enhver har ret til aktindsigt i domme og kendelser mv., ligesom den, der har en individuel, væsentlig interesse i et konkret retsspørgsmål, som udgangspunkt kan forlange at blive gjort bekendt med dokumenter, der vedrører en straffesag, herunder indførsler i retsbøgerne, i det omfang dokumenterne har betydning for vurderingen af det pågældende retsspørgsmål. Herudover indeholder retsplejeloven regler om berigtigelse af retsafgørelser.

2.4.1.4. Persondatalovens §§ 35 og 37 indeholder regler om den registreredes ret til indsigelse, berigtigelse, blokering og sletning af personoplysninger.

Det fremgår således af § 35, at den registrerede til enhver tid over for den dataansvarlige kan gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling. Hvis indsigelsen efter stk. 1 er berettiget, må behandlingen ikke længere omfatte de pågældende oplysninger, jf. stk. 2.

Det fremgår videre af persondatalovens § 37, at den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Det fremgår af retsplejelovens § 221, stk. 1, at retten til enhver tid i embeds medfør eller ifølge begæring kan berigtige skrivefejl, som er indløbet i henseende til ord, navne eller tal, blotte regnefejl samt sådanne fejl og forglemmelser, som alene vedrører udfærdigelsens form. Øvrige fejl og forglemmelser kan berigtiges, hvis parterne ikke udtaler sig herimod.

Retten kan også, når begæring derom fremkommer inden ankefristens udløb, og efter at der er givet parterne og i straffesager tillige forsvareren lejlighed til at ytre sig derom, berigtige den i afgørelsen af en borgerlig sag indeholdte fremstilling af parternes mundtlige angivelser og ytringer eller den i afgørelsen af en straffesag indeholdte fremstilling af sagens faktiske sammenhæng, for så vidt fremstillingen erkendes at lide af fejl, bestående i forbigåelser, uklarheder eller modsigelser, men derimod ikke i øvrigt foretage forandringer enten i begrundelsen eller resultatet. Beslutning angående slige berigtigelser træffes, og meddelelse om dem sker efter de samme regler, som gælder for den oprindelige afgørelse, jf. retsplejelovens § 221, stk. 2.

2.4.2. Retshåndhævelsesdirektivet

Direktivets kapitel III indeholder regler om oplysninger, der stilles til rådighed eller gives til den registrerede (artikel 13), den registreredes indsigtsret og begrænsninger heraf (artiklerne 14 og 15), retten til berigtigelse, sletning og begrænsning af behandling (artikel 16) samt generelle regler om udøvelsen af disse rettigheder (artiklerne 17 og 18).

2.4.2.1. Efter direktivets artikel 13 skal den dataansvarlige som minimum stille en række nærmere angivne oplysninger til rådighed for den registrerede, herunder identitet på og kontaktoplysninger for den dataansvarlige, kontaktoplysninger for en eventuel databeskyttelsesrådgiver og formålene med den behandling, som personoplysningerne skal bruges til.

Det fremgår af direktivets præambelbetragtning nr. 42, at dette kan ske på den kompetente myndigheds websted.

Den dataansvarlige skal herudover i særlige tilfælde give den registrerede yderligere en række oplysninger, for at vedkommende kan udøve sine rettigheder, herunder retsgrundlaget for behandlingen og det tidsrum, hvor personoplysningerne vil blive opbevaret, eller, hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum, jf. herved nærmere direktivets artikel 13, stk. 2.

Der kan efter artikel 13, stk. 3, i visse situationer ske udsættelse, begrænsning eller afskæring af meddelelse af oplysninger til de registrerede. Det kan ske for at undgå, at der lægges hindringer i vejen for officielle eller retlige undersøgelser, efterforskninger eller procedurer, undgå at skade forebyggelsen, afsløringen, efterforskningen eller retsforfølgningen af strafbare handlinger eller fuldbyrdelsen af strafferetlige sanktioner, beskytte den offentlige sikkerhed, beskytte statens sikkerhed eller beskytte andres rettigheder og frihedsrettigheder. Efter bestemmelsens stk. 4 kan der fastsættes nærmere regler om de kategorier af behandling, som helt eller delvis er omfattet af stk. 3.

2.4.2.2. Den registrerede har efter artikel 14 ret til at få den dataansvarliges bekræftelse på, om personoplysninger vedrørende den pågældende behandles, og i givet fald adgang til personoplysningerne og en række nærmere angivne oplysninger, herunder formålene med og retsgrundlaget for behandlingen og de berørte kategorier af personoplysninger.

Det fremgår af direktivets præambelbetragtning nr. 43, at en fysisk person bør have ret til indsigt i oplysninger, 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. Enhver registreret bør derfor navnlig have ret til at kende og blive underrettet om de formål, hvortil oplysningerne behandles, perioden, hvor oplysningerne behandles, og modtagerne af oplysningerne, herunder sådanne i tredjelande. Når sådan en underretning omfatter meddelelse om personoplysningernes oprindelse, bør oplysningerne ikke afsløre identiteten på fysiske personer, navnlig fortrolige kilder. Med henblik på overholdelse af denne ret er det tilstrækkeligt, at den registrerede er i besiddelse af et fuldstændigt resumé af disse oplysninger i en letforståelig form, det vil sige en form, der giver den pågældende registrerede mulighed for at blive opmærksom på disse oplysninger og kontrollere, at de er korrekte og behandlet i overensstemmelse med dette direktiv, så det er muligt for den pågældende at udøve de rettig-

heder, der tilkommer vedkommende i henhold til dette direktiv. Et sådant resumé kan have form af en kopi af de personoplysninger, der behandles.

Den registreredes ret til indsigt kan efter omstændighederne begrænses efter artikel 15 for at undgå, at der lægges hindringer i vejen for officielle eller retlige undersøgelser, efterforskninger eller procedurer, undgå at skade forebyggelsen, afsløringen, efterforskningen eller retsforfølgningen af strafbare handlinger eller fuldbyrdelsen af strafferetlige sanktioner, beskytte den offentlige sikkerhed, beskytte statens sikkerhed, eller beskytte andres rettigheder og frihedsrettigheder. Efter bestemmelsens stk. 2 kan der fastsættes nærmere regler om de kategorier af behandling, som helt eller delvis er omfattet af stk. 1.

Efter artikel 15, stk. 3, skal den dataansvarlige i de i stk. 1 og 2 omhandlede tilfælde uden unødig forsinkelse give den registrerede skriftlig meddelelse om ethvert afslag på indsigt i personoplysninger eller begrænsning af indsigten og om begrundelsen for afslaget eller begrænsningen. En sådan meddelelse kan udelades, hvis sådanne oplysninger ville være til skade for et af formålene i stk. 1. Den dataansvarlige skal underrette den registrerede om muligheden for at indgive en klage til en tilsynsmyndighed eller adgangen til retsmidler.

Den dataansvarlige skal dokumentere den faktiske eller retlige begrundelse, som afgørelsen hviler på. Disse oplysninger stilles til rådighed for tilsynsmyndighederne, jf. stk. 4.

2.4.2.3. Det fremgår af direktivets artikel 16, stk. 1, at den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. Den registrerede skal under hensyntagen til formålene med behandlingen have ret til at få fuldstændiggjort ufuldstændige personoplysninger, bl.a. ved at fremlægge en supplerende erklæring.

Det fremgår af direktivets præambelbetragtning nr. 47, at retten til berigtigelse imidlertid ikke bør berøre eksempelvis indholdet af et vidneudsagn.

Den dataansvarlige skal slette personoplysninger uden unødig forsinkelse, og den registrerede skal have ret til at få personoplysninger om sig selv slettet af den dataansvarlige uden unødig forsinkelse, hvis behandling overtræder de bestemmelser, der vedtages i henhold til artikel 4 (behandlingsprincipper), 8 (behandling af almindelige oplysninger) eller 10 (be-

handling af særlige kategorier af oplysninger), eller hvis personoplysninger skal slettes for at overholde en retlig forpligtelse, som den dataansvarlige er underlagt, jf. artikel 16, stk. 2.

Det fremgår videre af bestemmelsens stk. 3, at i stedet for sletning begrænser den dataansvarlige behandlingen, hvis rigtigheden af personoplysningerne bestrides af den registrerede og deres rigtighed eller urigtighed ikke kan konstateres, eller personoplysningerne skal bevares som bevismiddel. Hvis behandling er begrænset som følge af, at rigtigheden af personoplysningerne bestrides af den registrerede og deres rigtighed eller urigtighed ikke kan konstateres, underretter den dataansvarlige den registrerede herom, inden begrænsningen af behandling ophæves.

Det fremgår af direktivets præambelbetragtning nr. 47, at en fysisk person også bør have ret til begrænsning af behandlingen, hvis vedkommende bestrider personoplysningers rigtighed, og det ikke kan konstateres, om oplysningerne er rigtige eller ej, eller hvis personoplysningerne skal bevares som bevismiddel. I stedet for at slette personoplysninger bør behandling navnlig begrænses, hvis der i et konkret tilfælde er rimelig grund til at tro, at sletning vil kunne påvirke den registreredes legitime interesser. I så fald bør begrænsede oplysninger kun behandles til det formål, der gjorde, at de ikke blev slettet. Metoderne til at begrænse behandlingen af personoplysninger kan bl.a. omfatte, at udvalgte oplysninger flyttes til et andet behandlingssystem, f.eks. til arkivformål, eller at udvalgte oplysninger gøres utilgængelige. I automatiske registre bør behandling i princippet begrænses ved hjælp af tekniske hjælpemidler. Det forhold, at behandlingen af personoplysningerne er begrænset, bør angives i registret på en sådan måde, at det tydeligt fremgår, at behandlingen af personoplysningerne er begrænset. En sådan berigtigelse eller sletning af personoplysninger eller begrænsning af behandling bør meddeles de modtagere, hvortil oplysningerne er videregivet, og de kompetente myndigheder, hvorfra de urigtige oplysninger stammer. Den dataansvarlige bør også afstå fra yderligere udbredelse af sådanne oplysninger.

Efter bestemmelsens stk. 4 skal den dataansvarlige give den registrerede skriftlig meddelelse om ethvert afslag på berigtigelse eller sletning af personoplysninger eller begrænsning af behandling og om begrundelsen for afslaget.

Forpligtelsen til at give sådanne oplysninger kan i visse situationer helt eller delvist begrænses for at undgå, at der lægges hindringer i vejen for

officielle eller retlige undersøgelser, efterforskninger eller procedurer, undgå at skade forebyggelsen, afsløringen, efterforskningen eller retsforfølgningen af strafbare handlinger eller fuldbyrdelsen af strafferetlige sanktioner, beskytte den offentlige eller statens sikkerhed og beskytte andres rettigheder og frihedsrettigheder. Den dataansvarlige skal underrette den registrerede om muligheden for at indgive klage til en tilsynsmyndighed eller adgangen til retsmidler.

Den dataansvarlige skal meddele berigtigelse af urigtige personoplysninger til den kompetente myndighed, hvorfra de urigtige oplysninger stammer, jf. bestemmelsens stk. 5.

Endeligt fremgår det af bestemmelsens stk. 6, at den dataansvarlige skal underrette modtagerne, hvis personoplysningerne er blevet berigtiget eller slettet eller behandlingen er blevet begrænset, jf. stk. 1, 2 og 3, og at modtagerne skal berigtige eller slette personoplysningerne eller begrænse behandling af personoplysninger, som de har ansvaret for.

2.4.2.4. Direktivets artikel 12 indeholder en række regler om, hvordan den dataansvarlige skal behandle anmodninger fra den registrerede, herunder om hvordan de ovennævnte oplysninger og meddelelser skal gives, samt om udøvelsen af den registreredes rettigheder.

Det fremgår af stk. 1, at den dataansvarlige skal iværksætte rimelige tiltag for at give enhver oplysning som omhandlet i artikel 13 og enhver meddelelse som omhandlet i artikel 11, 14-18 og 31 om behandling til den registrerede i en kortfattet, letforståelig og lettilgængelig form og i et klart og enkelt sprog. Oplysningerne gives på enhver hensigtsmæssig måde, herunder ved hjælp af elektroniske midler. Som hovedregel skal den dataansvarlige give oplysningerne i samme form som anmodningen.

Den dataansvarlige skal lette udøvelsen af den registreredes rettigheder i medfør af artikel 11 og 14-18, jf. artikel 12, stk. 2.

Efter bestemmelsens stk. 3 skal den dataansvarlige give den registrerede skriftlig meddelelse om opfølgningen på dennes anmodning uden unødig forsinkelse.

Det fremgår videre af bestemmelsens stk. 4, at de oplysninger, der gives i medfør af artikel 13, og enhver meddelelse og enhver foranstaltning, der træffes i henhold til artikel 11, 14-18 og 31, er gratis. Hvis anmodninger

fra en registreret er åbenbart grundløse eller overdrevne, især fordi de gentages, kan den dataansvarlige enten opkræve et rimeligt gebyr under hensyntagen til de administrative omkostninger ved at give oplysninger eller meddelelser eller træffe den ønskede foranstaltning, eller afvise at efterkomme anmodningen. Bevisbyrden for, at anmodningen er åbenbart grundløs eller overdreven, påhviler den dataansvarlige.

Den dataansvarlige kan, hvis der hersker rimelig tvivl om identiteten af den fysiske person, der fremsætter en anmodning som omhandlet i artikel 14 eller 16, anmode om de yderligere oplysninger, der er nødvendige for at bekræfte den registreredes identitet, jf. stk. 5.

Efter direktivets artikel 17, stk. 1, kan den registrerede udøve sine rettigheder efter artikel 13, stk. 3, artikel 15, stk. 3, og artikel 16, stk. 4, gennem den kompetente tilsynsmyndighed.

Den dataansvarlige skal underrette den registrerede om dennes mulighed for at udøve sine rettigheder gennem tilsynsmyndigheden, jf. artikel 17, stk. 2.

Efter artikel 17, stk. 3, skal tilsynsmyndigheden i givet fald som minimum underrette den registrerede om, at tilsynsmyndigheden har foretaget den nødvendige kontrol eller undersøgelse. Tilsynsmyndigheden underretter også den registrerede om dennes adgang til retsmidler.

Det fremgår endeligt af direktivets artikel 18, at medlemsstaterne kan fastsætte bestemmelser om, at udøvelsen af de rettigheder, der er omhandlet i artikel 13, 14 og 16, skal gennemføres i henhold til medlemsstaternes nationale ret, når personoplysningerne er indeholdt i en retsafgørelse eller et register eller en sagsakt, der behandles i forbindelse med strafferetlige efterforskninger og straffesager.

Det fremgår af direktivets præambelbetragtning nr. 49, at hvis personoplysningerne behandles under en strafferetlig efterforskning og strafferetssag, bør medlemsstaterne kunne fastsætte bestemmelser om, at udøvelsen af retten til oplysninger, indsigt i og berigtigelse eller sletning af personoplysninger og begrænsning af behandling skal udføres i henhold til de nationale retsplejeregler.

2.4.3. Justitsministeriets overvejelser og lovforslagets udformning

2.4.3.1. Direktivets artikel 13 indeholder regler om de oplysninger, som den dataansvarlige skal stille til rådighed for eller meddele den registrerede.

Persondatalovens regler om oplysningspligt over for den registrerede finder ikke anvendelse for politiets, anklagemyndighedens og domstolenes behandling af personoplysninger på det strafferetlige område. Heller ikke rammeafgørelsesbekendtgørelsen indeholder en sådan forpligtelse for disse myndigheder.

Det foreslås på den baggrund, at der i overensstemmelse med direktivets artikel 13, stk. 1, fastsættes en regel om, at den dataansvarlige skal stille de oplysninger, der er nævnt i direktivet, til rådighed for den registrerede.

Den dataansvarliges forpligtelse til at stille oplysninger til rådighed kan f.eks. opfyldes ved at gøre oplysningerne tilgængelige på den kompetente myndigheds hjemmeside eller gennem trykt materiale, som er tilgængeligt for de registrerede.

Det foreslås endvidere, at der i overensstemmelse med direktivets artikel 13, stk. 2 og 3, fastsættes regler om, at den dataansvarlige i særlige tilfælde skal give den registrerede meddelelse om de oplysninger, der er nævnt i direktivets artikel 13, stk. 2, med mindre der foreligger en af de grunde, der er nævnt i direktivets artikel 13, stk. 3.

Der henvises i øvrigt til lovforslagets § 13 og bemærkningerne hertil.

2.4.3.2. Direktivets artikel 14 indeholder regler om den registreredes indsigtsret.

Persondatalovens regler om den registreredes indsigtsret finder anvendelse for de kompetente myndigheder med undtagelse af domstolene, som dog er omfattet heraf for så vidt angår behandling, der er omfattet af rammeafgørelsesbekendtgørelsen.

Den dataansvarlige er forpligtet til at give den registrerede flere oplysninger efter retshåndhævelsesdirektivet end efter persondatalovens regler.

Det foreslås på den baggrund, at der i overensstemmelse med direktivets artikel 14 fastsættes en regel om, at den dataansvarlige efter anmodning fra

den registrerede skal give den pågældende de oplysninger, der er nævnt i direktivet.

Direktivets artikel 15 indeholder regler om begrænsning af indsigtsretten. Reglerne svarer i vidt omfang til de gældende regler i persondataloven, idet hensynet til den registrerede selv dog ikke efter direktivet kan begrunde en begrænsning.

Efter Justitsministeriets opfattelse vil det imidlertid være hensigtsmæssigt, hvis det også fremover er muligt for den dataansvarlige at begrænse indsigtsretten af hensyn til den registrerede selv, hvilket navnlig kan være relevant for de registrerede, som har berøring med kriminalforsorgen. En sådan udvidelse af adgang til at begrænse indsigtsretten er efter Justitsministeriets opfattelse i overensstemmelse med direktivet, idet der er tale om udvidelse af beskyttelsen af den registreredes rettigheder, jf. direktivets artikel 1, stk. 3.

Det foreslås på den baggrund, at der i overensstemmelse med direktivets artikel 15 fastsættes en regel om, at indsigtsretten kan begrænses af de grunde, der er nævnt i direktivet med den ovennævnte tilføjelse.

Direktivets artikel 18 giver mulighed for, at medlemsstaterne kan bestemme, at udøvelsen af bl.a. indsigtsretten kan ske gennem de nationale retsplejeregler. Retsplejelovens regler om adgangen til indsigt i retsafgørelser indeholder efter Justitsministeriets opfattelse de rettigheder, som fremgår af direktivets artikel 14. Det foreslås på den baggrund, at den registreredes anmodning om indsigt i oplysninger om den pågældende i retsafgørelser skal ske efter retsplejelovens regler.

Der henvises i øvrigt til lovforslagets § 15, § 16 og § 18, stk. 3, og bemærkningerne hertil.

2.4.3.3. Retshåndhævelsesdirektivets artikel 16 indeholder regler om den registreredes ret til berigtigelse, sletning og begrænsning af behandling.

Persondatalovens regler om den registreredes ret til indsigelse, berigtigelse, blokering og sletning af personoplysninger finder ikke anvendelse for politiets, anklagemyndighedens og domstolenes behandling af personoplysninger i straffesager. Persondatalovens § 37 om berigtigelse mv. finder dog anvendelse i forhold til den behandling, som er omfattet af rammeafgørelsesbekendtgørelsen, jf. bekendtgørelsens § 2, stk. 4.

Det foreslås på den baggrund, at der i overensstemmelse med direktivets artikel 16 fastsættes en regel om, at den dataansvarlige efter anmodning fra den registrerede skal berigtige eller slette oplysninger om den pågældende, eller – hvis de grunde, der er nævnt i direktivet, er opfyldt – begrænse behandlingen heraf. Af de grunde, som er nævnt ovenfor i pkt. 2.4.3.2 foreslås det endvidere, at udøvelsen af retten til berigtigelse mv. i forhold til personoplysninger i retsafgørelser skal ske efter retsplejelovens regler.

Der henvises i øvrigt til lovforslagets § 15 og § 17, og § 18, stk. 3, og bemærkningerne hertil.

2.4.3.4. Direktivets artikel 12 indeholder en række generelle regler om den registreredes udøvelse af sine rettigheder og om formen for de meddelelser, som den dataansvarlige skal give til den registrerede.

Direktivets artikel 12, stk. 2, indeholder et krav om, at den dataansvarlige skal lette udøvelsen af den registreredes rettigheder i medfør af artikel 11 og 14-18.

Det foreslås på den baggrund, at der fastsættes et krav om, at den dataansvarlige skal lette udøvelsen af den registreredes rettigheder. Det vil f.eks. kunne ske ved, at den dataansvarlige udarbejder en særlig blanket, som den registrerede kan gøre brug af.

Direktivets artikel 12, stk. 3, indeholder et krav om, at den dataansvarlige skal give den registrerede skriftlig meddelelse om opfølgningen på dennes anmodning uden unødig forsinkelse.

Reglen er i vidt omfang sammenfaldende med persondatalovens § 31, stk. 2, om den dataansvarliges forpligtelser i forhold til behandlingen af en indsigtsanmodning, hvor der er fastsat en frist på 4 uger, inden for hvilken den dataansvarlige skal besvare anmodningen eller underrette den registrerede om grunden til en manglende besvarelse. Denne ordning er efter Justitsministeriets opfattelse i overensstemmelse med direktivets krav om meddelelse uden unødigt ophold, og den gældende ordning foreslås på den baggrund videreført.

Direktivets artikel 12, stk. 4, indeholder et krav om, at meddelelser mv. skal være gratis, og en mulighed for, at den dataansvarlige kan afvise eller

opkræve gebyr for behandlingen anmodninger, som er åbenbart grundløse eller overdrevne, især fordi de gentages.

Den foreslåede ordning indeholder ikke en mulighed for at opkræve gebyr, hvorfor meddelelser mv. vil være gratis for de registrerede. I forhold til spørgsmålet om håndteringen af åbenlyst grundløse eller overdrevent gentagne anmodninger er det efter Justitsministeriets opfattelse mest hensigtsmæssigt at give de dataansvarlige myndigheder mulighed for at afvise sådanne anmodninger. En sådan ordning vil således i praksis være en videreførelse af persondatalovens § 33.

Persondataloven indeholder forskellige krav til, hvordan den dataansvarlige skal give meddelelser efter loven til den registrerede, herunder et krav om, at den dataansvarlige skal give meddelelser til den registrerede som følge af den pågældendes udøvelse af sin indsigtsret på en letforståelig måde. En del af de krav, som følger af direktivet må således anses for allerede at følge af gældende ret.

For at sikre, at der ikke kan opstå tvivl om, hvorvidt der er sket en korrekt implementering af direktivet, foreslås det imidlertid, at der i overensstemmelse med direktivets artikel 12 fastsættes de krav til meddelelsernes form mv., som følger af direktivet.

Det bemærkes i den forbindelse, at de kompetente myndigheders kommunikation med borgere også på dette område kan ske ved hjælp af offentlig Digital Post i overensstemmelse med reglerne i lovbekendtgørelse nr. 801 af 13. juni 2016 om Digital Post fra offentlige afsendere.

Der henvises i øvrigt til lovforslagets §§ 18 og 19 og bemærkningerne hertil.

2.5. Forpligtelser for den dataansvarlige og databehandleren

2.5.1. Gældende ret

2.5.1.1. Persondatalovens regler om den dataansvarliges og databehandlerens forpligtelse til at træffe tekniske og organisatoriske sikkerhedsforanstaltninger og kravene i forbindelse med den dataansvarliges overladelse af en behandling af personoplysninger til en databehandler er knyttet til reglerne om behandlingssikkerhed, jf. pkt. 2.6.1 nedenfor.

2.5.1.2. Persondataloven indeholder ikke krav om, at den dataansvarlige skal føre fortegnelser over eller foretage logning af behandlingsaktiviteter.

Justitsministeren har imidlertid med hjemmel i persondatalovens § 41, stk. 5, udstedt bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen), og bekendtgørelse nr. 535 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for domstolene (sikkerhedsbekendtgørelsen for domstolene), som indeholder regler om logning.

Det fremgår således af § 19, jf. § 2, stk. 2, i sikkerhedsbekendtgørelsen, at der skal foretages maskinel registrering (logning) af alle anvendelser af fortrolige personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Det fremgår videre af bestemmelsens stk. 2, at stk. 1 ikke finder anvendelse for personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form. Det samme gælder sådanne dokumenter, som foreligger i endelig form, hvis der sker sletning inden for en af den dataansvarlige myndighed nærmere fastsat kortere frist.

Bestemmelsen i stk. 1 finder heller ikke anvendelse, hvis behandlingen af personoplysninger udelukkende sker ved afvikling af programmer, som foretager en forud defineret massebehandling af personoplysninger (batchkørsler). Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen, jf. stk. 3.

Bestemmelsen i stk. 1 finder endvidere ikke anvendelse, hvis behandlingen af personoplysningerne udelukkende sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med et kodenummer eller lignende. Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen, jf. stk. 4.

Bestemmelsen i stk. 1 finder endelig ikke anvendelse for personoplysninger, som i form af måle- eller analyseresultater automatisk lagres i medicoteknisk udstyr. Undtagelsen omfatter tillige personoplysninger, som manu-

elt registreres i medicoteknisk udstyr til supplering af automatisk lagrede oplysninger, jf. stk. 5.

Sikkerhedsbekendtgørelsen for domstolene indeholder i § 19 regler svarende til de ovennævnte regler i sikkerhedsbekendtgørelsens § 19, stk. 1, 2 og 4.

Rammeafgørelsesbekendtgørelsens § 10 indeholder et krav om, at den dataansvarlige med henblik på at kontrollere, om databehandlingen er lovlig, samt med henblik på at udøve egenkontrol og sikre integritet og sikkerhed skal registrere eller dokumentere hver videregivelse af personoplysninger.

Registreringen eller dokumentationen skal bl.a. indeholde oplysninger om, til hvilke organer der er blevet eller kan være blevet videregivet eller stillet personoplysninger til rådighed ved hjælp af datakommunikationsudstyr, og hvilke personoplysninger der er indlæst i edb-systemerne, hvornår og af hvem.

Registreringer, der foretages, eller dokumentation, der udarbejdes, videregives til Datatilsynet på dennes anmodning med henblik på kontrol af databeskyttelsen. For domstolenes vedkommende sker videregivelsen til Domstolsstyrelsen. Datatilsynet og Domstolsstyrelsen anvender kun disse oplysninger med henblik på kontrol af databeskyttelsen og med henblik på at sikre en korrekt databehandling og dataenes integritet og sikkerhed, jf. § 10, stk. 2.

2.5.1.3. Persondataloven indeholder ikke et krav om, at den dataansvarlige skal udarbejde konsekvensanalyser eller foretage forudgående høring af tilsynsmyndigheden.

Persondatalovens kapitel 12 (§§ 43-47) indeholder dog regler om anmeldelse af behandlinger, der foretages for den offentlige forvaltning, til tilsynsmyndigheden, jf. pkt. 2.6.1.2 nedenfor.

2.5.1.4. Spørgsmålet om fælles dataansvarlige er ikke direkte reguleret i persondataloven. Det følger imidlertid af definitionen af begrebet "den dataansvarlige" i persondatalovens § 3, nr. 4, at dette kan være en fysisk eller juridisk person, offentlig myndighed institution eller ethvert andet organ, der alene eller *sammen med andre* afgør, til hvilket formål og med hvilke virkemidler der må foretages behandling af oplysninger.

Spørgsmålet om fordelingen af ansvar og forpligtelser for de fælles dataansvarliges er ikke reguleret direkte i gældende ret. I sager, hvor Datatilsynet har accepteret et fælles dataansvar, har tilsynet imidlertid lagt til grund, at der skal foreligge klare retningslinjer og instruktionsbeføjelser for så vidt angår behandlingen af oplysninger. Herudover skal de registrerede kunne gøre deres rettigheder efter persondatalovens kapitel III, såsom retten til indsigt, oplysninger mv., gældende over for enhver af de fælles dataansvarlige.

2.5.2. Retshåndhævelsesdirektivet

2.5.2.1. Direktivets artikel 19 indeholder regler om den dataansvarliges pligter. Det fremgår således af bestemmelsens stk. 1, at den dataansvarlige under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med direktivet. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

Det fremgår videre af bestemmelsens stk. 2, at hvis det står i rimeligt forhold til behandlingsaktiviteterne, skal de foranstaltninger, der er omhandlet i stk. 1, omfatte den dataansvarliges implementering af passende databeskyttelsespolitikker.

Direktivets artikel 20 indeholder nærmere regler om databeskyttelse gennem design og gennem standardindstillinger. Det fremgår af bestemmelsens stk. 1, at den dataansvarlige 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, både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen skal gennemføre 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 dette direktiv og beskytte de registreredes rettigheder.

Det fremgår videre af artikel 20, stk. 2, at den dataansvarlige skal gennemføre 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 fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.

Direktivets artikel 21 indeholder regler om fælles dataansvarlige. Hvis to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til behandling, er de fælles dataansvarlige. De fastsætter på en gennemsigtig måde deres respektive ansvar for overholdelse af dette direktiv, navnlig hvad angår udøvelsen af den registreredes rettigheder og deres respektive forpligtelser til at fremlægge de oplysninger, der er omhandlet i artikel 13, ved hjælp af en ordning mellem dem, medmindre og i det omfang de dataansvarliges respektive ansvar er fastlagt i EU-retten eller medlemsstaternes nationale ret, som de dataansvarlige er underlagt. I ordningen udpeges kontaktpunktet for de registrerede.

Medlemsstaterne har herudover adgang til at fastsætte forskellige regler om ordningen for fælles dataansvarlige.

2.5.2.2. Direktivets artikel 22 indeholder regler om databehandleren.

Den dataansvarlige må udelukkende benytte databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i dette direktiv og sikrer beskyttelse af den registreredes rettigheder, jf. stk. 1.

Databehandlerens behandling skal ske på baggrund af en skriftlig kontrakt eller et andet bindende retsgrundlag, som skal fastsætte den dataansvarliges pligter og rettigheder, herunder at den dataansvarlige kun må handle på instruks fra den dataansvarlige og på forskellige måder skal bistå den dataansvarlige med at overholde reglerne om den registreredes rettigheder mv., jf. nærmere herom i direktivets artikel 22, stk. 3.

En databehandlers anvendelse af en anden databehandler skal ske på baggrund af en skriftlig aftale, og i visse situationer skal databehandleren underrette den dataansvarlige om, at der anvendes andre databehandlere, jf. nærmere herom i direktivets artikel 22, stk. 2.

Agerer en databehandler som en dataansvarlig, dvs. fastsætter formål med og hjælpemidler til behandling, omfattes databehandleren af reglerne om de dataansvarlige, jf. artikel 22, stk. 5.

Databehandleren og enhver, der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, må kun behandle disse oplysninger efter instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret, jf. direktivets artikel 23.

2.5.2.3. Direktivets artikel 24 indeholder regler om fortegnelser over behandlingsaktiviteter.

Den dataansvarlige skal føre fortegnelser over alle kategorier af behandlingsaktiviteter under deres ansvar. Direktivet indeholder en liste over de oplysninger, som fortegnelserne skal indeholde, herunder navn på og kontaktoplysninger for den dataansvarlige og, hvis det er relevant, den fælles dataansvarlige og databeskyttelsesrådgiveren, formålene med behandlingen, og en angivelse af retsgrundlaget for behandlingsaktiviteten, herunder overførsler, hvortil personoplysningerne er bestemt, jf. nærmere herom i direktivets artikel 24, stk. 1. På tilsvarende måde skal databehandlere føre fortegnelser, som skal indeholde en række oplysninger, som knytter sig til databehandlerens funktion, jf. nærmere herom i direktivets artikel 24, stk. 2.

Efter direktivets artikel 25, stk. 1, skal der som minimum foretages logning af følgende former for behandlingsaktiviteter i automatiske databehandlingssystemer: indsamling, ændring, søgning, videregivelse, herunder overførsel, samkøring og sletning. Logning af søgning og videregivelse skal gøre det muligt at fastlægge begrundelsen, datoen og tidspunktet for sådanne aktiviteter og i videst muligt omfang identifikation af den person, som har søgt eller videregivet personoplysninger, og identiteten på modtagerne af sådanne personoplysninger.

Det fremgår videre af bestemmelsens stk. 2, at loggene udelukkende anvendes til at kontrollere, om behandling er lovlig, til egenkontrol, til at sikre integriteten og sikkerheden af personoplysningerne og i forbindelse med straffesager.

Det fremgår endeligt af bestemmelsens stk. 3, at den dataansvarlige og databehandleren efter anmodning stiller loggene til rådighed for tilsynsmyndigheden.

Det fremgår af direktivets præambelbetragtning nr. 57, at der som minimum bør ske logning af aktiviteter i automatiske databehandlingssystemer såsom indsamling, ændring, søgning, videregivelse, herunder overførsel, samkøring eller sletning. Navnet på den person, som har søgt eller videregivet personoplysninger, bør logges, og herudfra bør det være muligt at fastlægge begrundelsen for behandlingsaktiviteterne. Loggene bør udelukkende anvendes til at kontrollere, om databehandlingen er lovlig, til egenkontrol, til at sikre dataintegriteten og datasikkerheden og i forbindelse med straffesager. Egenkontrol omfatter også kompetente myndigheders interne disciplinærsager.

Direktivets artikel 63, stk. 2 og 3, indeholder særlige regler om anvendelsestidspunktet for direktivets artikel 25 om logning. Det fremgår således af artikel 63, stk. 2, at medlemsstaterne i ekstraordinære tilfælde, og hvis det er uforholdsmæssigt vanskeligt, kan fastsætte bestemmelser om, at automatiske behandlingssystemer, der er indført før den 6. maj 2016, skal bringes i overensstemmelse med artikel 25, stk. 1, senest den 6. maj 2023.

Det fremgår videre af bestemmelsens stk. 3, at en medlemsstat under ekstraordinære omstændigheder kan bringe et automatisk behandlingssystem som omhandlet i stk. 2 i overensstemmelse med artikel 25, stk. 1, inden for en nærmere angivet periode efter den 6. maj 2023, hvis det i modsat fald ville forårsage alvorlige vanskeligheder for driften af det pågældende automatiske behandlingssystem. Medlemsstaten meddeler Kommissionen årsagerne til disse alvorlige vanskeligheder og årsagerne til den angivne periode, inden for hvilken den bringer det pågældende automatiske behandlingssystem i overensstemmelse med artikel 25, stk. 1. Den angivne periode må under ingen omstændigheder være senere end den 6. maj 2026.

Fortegnelserne, som skal foreligge skriftligt, herunder elektronisk, og loggene skal stilles til rådighed for tilsynsmyndigheden, jf. artikel 24, stk. 2, og artikel 25, stk. 3, ligesom den dataansvarlige og databehandleren i øvrigt skal samarbejde med tilsynsmyndigheden, jf. artikel 26.

2.5.2.4. Direktivets artikel 27 og 28 indeholder regler om henholdsvis konsekvensanalyser og forudgående høring af tilsynsmyndigheden.

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, skal den dataansvarlige forud for behandlingen foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger, jf. direktivets artikel 27, stk. 1.

Analysen skal mindst omfatte en generel beskrivelse af de planlagte behandlingsaktiviteter, en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder de foranstaltninger, der påtænkes for at imødegå disse risici, garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af dette direktiv, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser, jf. bestemmelsens stk. 2.

Det fremgår af direktivets præambelbetragtning nr. 58, at konsekvensanalyser bør omfatte behandlingsaktiviteters relevante systemer og processer, men ikke enkeltsager.

Efter direktivets artikel 28 skal den dataansvarlige eller databehandleren høre tilsynsmyndigheden inden behandling af personoplysninger, der vil indgå som en del af et nyt register, der skal oprettes, såfremt en konsekvensanalyse vedrørende databeskyttelse, jf. artikel 27, viser, at behandlingen vil føre til en høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen, eller den type behandling, navnlig ved brug af nye teknologier, mekanismer eller procedurer, indebærer en høj risiko for de registreredes rettigheder og frihedsrettigheder. Tilsynsmyndigheden skal kunne fastsætte en liste over de behandlingsaktiviteter, hvor der skal ske forudgående høring, jf. bestemmelsens stk. 3.

Den dataansvarlige skal i forbindelse med høringen stille konsekvensanalysen og efter anmodning andre nødvendige oplysninger til rådighed for tilsynsmyndigheden, jf. artikel 28, stk. 4.

Hvis tilsynsmyndigheden finder, at den planlagte behandling overtræder de bestemmelser, der vedtages i henhold til direktivet, navnlig hvis den dataansvarlige ikke tilstrækkeligt har identificeret eller begrænset risikoen, skal tilsynsmyndigheden inden for en periode på op til seks uger efter modtagelsen 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. 6-ugers perioden kan forlænges

med en måned under hensyntagen til den påtænkte behandlings kompleksitet. Tilsynsmyndigheden giver underretning om og begrunder enhver sådan forlængelse senest en måned efter modtagelse af anmodningen om høring, jf. direktivets artikel 28, stk. 5.

Det fremgår af direktivets præambelbetragtning nr. 96, at hvis en behandling overholder den EU-ret, der er gældende inden datoen for direktivets ikrafttræden, bør kravene i dette direktiv om forudgående høring af tilsynsmyndigheden ikke finde anvendelse på de behandlingsaktiviteter, der allerede var iværksat på denne dato, idet disse krav i sagens natur skal opfyldes forud for behandlingen.

Direktivets artikel 28, stk. 2, indeholder herudover en regel om høring af tilsynsmyndigheden ved udarbejdelse af lovforslag og lignende, jf. nærmere om tilsynsmyndigheden i pkt. 2.9.2 nedenfor.

Endelig indeholder direktivets artikel 48 et krav om, at kompetente myndigheder skal indføre effektive mekanismer, som tilskynder til fortrolig indberetning af overtrædelser af direktivet.

2.5.3. Justitsministeriets overvejelser og lovforslagets udformning

Der er ikke i gældende ret en eksplicit og overordnet bestemmelse om den dataansvarliges ansvar. I stedet følger den dataansvarliges ansvar implicit af, at den dataansvarlige har retten til at disponere og bestemme over de pågældende personoplysninger og derfor også er ansvarlig for overholdelse af databeskyttelsesretten ved behandling af personoplysninger. Dette følger endvidere implicit af de krav og forpligtelser, som den dataansvarlige er underlagt efter gældende ret.

2.5.3.1. Direktivets artikel 19 indeholder krav om, at den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med direktivet. Der kan være tale om foranstaltninger, som er designet til eller gennem standardindstillinger opfylder disse krav, jf. direktivets artikel 20.

Retshåndhævelsesdirektivet indeholder således i princippet en nyskabelse på dette punkt, idet de tekniske og organisatoriske foranstaltninger, som de dataansvarlige i dag er forpligtede til at træffe, er knyttet til spørgsmålet om behandlingssikkerheden.

De gældende regler om behandlingssikkerhed må imidlertid i vidt omfang anses for at dække den forpligtelse, som følger af direktivets artikel 19, idet direktivet dog indeholder en særskilt forpligtelse til, at de trufne foranstaltninger skal gøre den dataansvarlige i stand til at påvise, at direktivet overholdes.

Persondataloven indeholder ikke bestemmelser, som specifikt kræver databeskyttelse gennem design eller databeskyttelse gennem standardindstillinger.

Persondatalovens § 41, stk. 3, forpligter imidlertid den dataansvarlige og databehandleren til at beskytte mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven.

Persondataloven fastsætter ingen nærmere tidsmæssig ramme for, hvornår foranstaltningerne skal være truffet. Foranstaltningerne vil dog som udgangspunkt altid skulle forberedes eller implementeres forud for, at behandlingen påbegyndes. Datatilsynets praksis indeholder eksempler på, at persondatalovens behandlingsbetingelser og sikkerhedskrav skal iagttages ved indretningen af digitale løsninger.

Direktivets krav om databeskyttelse gennem design eller databeskyttelse gennem standardindstillinger må på den baggrund helt overordnet anses for at være en videreførelse af gældende ret.

Det bemærkes i den forbindelse, at kravet om databeskyttelse gennem design og standardindstillinger efter Justitsministeriets opfattelse ikke stiller krav om, at eksisterende systemer skal redesignes. Kravene er således alene relevante i forhold til udvikling og design af fremtidige systemer.

For at sikre, at der ikke kan opstå tvivl om, hvorvidt der er sket en korrekt implementering af direktivet, foreslås det, at der i overensstemmelse med direktivets artikel 19 fastsættes et eksplicit krav om, at den dataansvarlige skal gennemføre de fornødne tekniske og organisatoriske foranstaltninger, og at dette kan ske gennem databeskyttelse gennem design eller standardindstillinger.

Der henvises i øvrigt til lovforslagets § 20 og bemærkningerne hertil.

2.5.3.2. Direktivets artikel 21 giver mulighed for, at flere dataansvarlige kan være fælles dataansvarlige.

Der er som nævnt ovenfor i pkt. 2.5.1.4 allerede i dag mulighed for, at flere dataansvarlige kan have et fælles dataansvar. Direktivets krav må derfor anses for at være en videreførelse af gældende ret.

Det foreslås på den baggrund, at der fastsættes en regel, hvorefter der i overensstemmelse med direktivets artikel 21 kan være fælles dataansvarlige.

Det bemærkes i den forbindelse, at kravet om, at de fælles dataansvarlige skal udpege et kontaktpunkt, kan opfyldes ved at udpege den eller de dataansvarliges databeskyttelsesrådgiver som kontaktpunkt.

Der henvises i øvrigt til lovforslagets § 21 og bemærkningerne hertil.

2.5.3.3. Direktivets artikel 22 indeholder regler om databehandleren og om kravene til det retlige forhold mellem den dataansvarlige og databehandleren.

Der stilles efter gældende ret de samme krav til databehandleren som til den dataansvarlige i forhold til de fornødne tekniske og organisatoriske foranstaltninger, jf. nedenfor i pkt. 2.6.1.1.

Retshåndhævelsesdirektivet indeholder imidlertid en nyskabelse i form af flere og mere detaljerede krav til indholdet i en databehandleraftale, og dermed til databehandlerens forpligtelser over for den dataansvarlige, end efter gældende ret. Herudover sker der en mere detaljeret regulering af den situation, hvor en databehandler ønsker at anvende en underdatabehandler.

Det foreslås på den baggrund, at der fastsættes en regel svarende til direktivets artikel 22, idet det dog præciseres, at en databehandler senest 14 dage forud for, at der sker overladelse af behandling til en underdatabehandler i medfør af en generel aftale med den dataansvarlige herom, skal underrette den dataansvarlige om overladelsen. Den dataansvarlige vil i den forbindelse kunne modsætte sig overladelsen, hvis det anses for nødvendigt.

Det bemærkes i forhold til spørgsmålet om databehandleraftaler, at de kompetente myndigheder tillige vil behandle personoplysninger i sager og med formål, som falder uden for det foreslåede anvendelsesområde for loven. Denne behandling vil i stedet være omfattet af persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen. Dette indebærer, at databehandleraftaler efter omstændighederne vil skulle overholde kravene i såvel retshåndhævelsesdirektivet som – efter den 25. maj 2018 – databeskyttelsesforordningen.

Det er imidlertid Justitsministeriets vurdering, at de krav til databehandlerne mv., som følger af henholdsvis retshåndhævelsesdirektivet og databeskyttelsesforordningen, ikke strider mod hinanden, og at en overholdelse af retshåndhævelsesdirektivet – som gennemført i denne lov – samtidig vil opfylde forordningens krav.

Der henvises i øvrigt til lovforslagets § 22 og bemærkningerne hertil.

2.5.3.4. Direktivets artikel 24 indeholder et krav om, at den dataansvarlige skal føre fortegnelser over alle kategorier af behandlingsaktiviteter.

Der følger ikke en eksplicit fortegnelsesforpligtelse efter gældende ret.

Det følger imidlertid af reglerne om anmeldelsespligten i persondatalovens kapitel 12, jf. pkt. 2.6.1.2, at der ved behandlinger, som er omfattet af disse forpligtelser, skal ske anmeldelse til tilsynsmyndigheden, og at anmeldelsen bl.a. skal indeholde en optegnelse over de behandlingsaktiviteter, der påtænkes iværksat.

Der følger således for så vidt et krav om fortegnelser over behandlingsaktiviteter i medfør af anmeldelsesforpligtelsen efter gældende ret.

Hvis en dataansvarlig er omfattet af det gældende anmeldelseskrav, vil den dataansvarlige således i vidt omfang kunne genanvende de anmeldelser, der er indsendt til Datatilsynet, til at opfylde direktivets krav om, at der skal føres fortegnelser over behandlingsaktiviteter.

For så vidt angår de behandlinger, der *ikke* er omfattet af anmeldelsespligten efter gældende ret, vil disse nu i medfør af artikel 24 skulle indgå i en fortegnelse, som omfatter al behandlingsaktivitet under den dataansvarliges ansvar. Også databehandlere pålægges fremover et fortegnelseskrav.

Den dataansvarlige er i allerede i dag forpligtet til at udlevere en oversigt over alle behandlinger – inklusiv de behandlingsaktiviteter, der ikke er omfattet af anmeldelsespligten – til enhver, der anmoder herom, jf. persondatalovens § 54, stk. 2. Dermed er den dataansvarlige i et vist omfang allerede omfattet af krav, der svarer til direktivets.

Der er derfor i praksis alene tale om en begrænset udvidelse af pligten til fortegnelse i artikel 24 i forhold til gældende ret for den dataansvarlige.

For databehandleren udvides pligten til fortegnelse i artikel 24 i forhold til gældende ret, idet alle behandlingsaktiviteter skal indgå i de elektroniske og skriftlige fortegnelser hos databehandleren.

Det foreslås på den baggrund, at der fastsættes en regel svarende til direktivets artikel 24.

Der henvises i øvrigt til lovforslagets § 23 og bemærkningerne hertil.

2.5.3.4. Direktivets artikel 25 indeholder et krav om logning af en række forskellige behandlingsaktiviteter. Allerede som følge af, at direktivets logningskrav ikke er begrænset til fortrolige oplysninger, er der tale om en udvidelse af den gældende forpligtelse i sikkerhedsbekendtgørelserne til at foretage logning. Det nærmere omfang af direktivets forpligtelse til at foretage logning giver imidlertid anledning til tvivl, herunder i forhold til spørgsmålet om, i hvilket omfang det i øvrigt vil være muligt at opretholde den gældende ordning for logning i sikkerhedsbekendtgørelserne.

2.5.3.4.1. Sikkerhedsbekendtgørelsen og sikkerhedsbekendtgørelsen for domstolene indeholder som nævnt ovenfor i pkt. 2.5.1.2 krav om, at der skal ske logning af behandling af fortrolige oplysninger.

Direktivets logningskrav kan imidlertid ikke isoleres til alene at angå fortrolige oplysninger. Der er således på dette punkt tale om en udvidelse af logningspligten. Udvidelsen skaber behov for at ændre i de automatiske databehandlingssystemer, som anvendes af de kompetente myndigheder i dag, og som alene er tilpasset kravet om logning i overensstemmelse med sikkerhedsbekendtgørelsens regler, herunder alene af fortrolige oplysninger. I overensstemmelse med direktivets artikel 63, stk. 2, foreslås det derfor, at tidspunktet for, hvornår logningskravet skal være opfyldt, udskydes, jf. nærmere herom nedenfor.

2.5.3.4.2. Som nævnt ovenfor giver det nærmere omfang af direktivets logningsforpligtelse anledning til tvivl, herunder i forhold til spørgsmålet om sammenhængen mellem henholdsvis direktivets og sikkerhedsbekendtgørelsernes logningskrav.

Det fremgår af artikel 25, stk. 1, 1. pkt., at der skal foretages logning af behandlingsaktiviteterne indsamling, ændring, søgning, videregivelse, herunder overførsel, samkøring og sletning.

Det fremgår videre af direktivets artikel 25, stk. 1, 2. pkt., at logning af alene behandlingsaktiviteterne søgning og videregivelse skal gøre det muligt at fastlægge begrundelsen, datoen og tidspunktet for sådanne aktiviteter og i videst muligt omfang identifikation af den person, som har søgt eller videregivet personoplysningerne, og identiteten på modtagerne af sådanne oplysninger.

For så vidt angår de øvrige behandlingsaktiviteter, der er omfattet af logningskravet efter artikel 25, stk. 1, 1. pkt., dvs. indsamling, ændring, samkøring og sletning, indeholder bestemmelsen ikke nærmere krav til logningen, og medlemsstaterne må således formentlig antages at have en højere grad af valgfrihed i forhold til, hvordan logningskravet skal udformes for så vidt angår disse behandlingsaktiviteter.

2.5.3.4.3. Som nævnt ovenfor fører udvidelsen af logningsforpligtelsen til, at der er behov for at ændre i de automatiske databehandlingssystemer, som anvendes af de retshåndhævende myndigheder i dag, og som alene er tilpasset kravet om logning i overensstemmelse med sikkerhedsbekendtgørelsens regler, herunder alene af fortrolige oplysninger. Der er allerede af den grund ikke teknisk mulighed for generelt at bringe de kompetente myndigheders automatiske databehandlingssystemer i overensstemmelse med direktivets logningskrav den 1. maj 2017.

Det kan – afhængig af en nærmere afklaring af logningskravets rækkevidde – ikke udelukkes, at visse af de automatiske databehandlingssystemer, som anvendes af de kompetente myndigheder i dag, vil kunne opfylde direktivets logningskrav inden for relativt kort tid. For andre systemers vedkommende vil en overholdelse af kravet imidlertid formentlig forudsætte mere omfattende ændringer.

I overensstemmelse med direktivets artikel 63, stk. 2, foreslås det derfor, at justitsministeren får bemyndigelse til at fastsætte nærmere regler om, hvil-

ke automatiske databehandlingssystemer logningskravet skal finde anvendelse på.

Denne ordning giver mulighed for, at der sammen med de kompetente myndigheder kan ske en nærmere afklaring af rækkevidden af logningsforpligtelsen, inden der tages initiativ til at ændre de kompetente myndigheders automatiske databehandlingssystemer.

Det sikres endvidere herved, at der vil kunne ske en løbende indfasning af forpligtelsen, eventuelt i forbindelse med at der sker udskiftning af eksisterende automatiske behandlingssystemer.

Logningskravet vil dog skulle finde anvendelse for alle relevante automatiske databehandlingssystemer senest den 6. maj 2023, eller, hvis det måtte vise sig, at direktivets logningskrav medfører alvorlige vanskeligheder for driften af de kompetente myndigheders automatiske behandlingssystemer, senest den 6. maj 2026.

Der henvises i øvrigt til lovforslagets § 24 og bemærkningerne hertil.

2.5.3.5. Direktivets artikler 27 og 28 indeholder regler om konsekvensanalyser og forudgående høring af tilsynsmyndigheden.

Direktivet indeholder en nyskabelse på dette punkt, idet der efter gældende ret ikke findes sådanne krav.

Det foreslås på den baggrund, at der i overensstemmelse med direktivets artikler 27 og 28 fastsættes regler om konsekvensanalyser og forudgående høring af tilsynsmyndigheden.

Det bemærkes i den forbindelse, at kravet om konsekvensanalyser og forudgående høring finder anvendelse på henholdsvis behandling, der foretages, og registre, der oprettes, den 1. maj 2017 eller senere, dvs. efter det foreslåede ikrafttrædelsestidspunkt, jf. også den foreslåede § 53 og bemærkninger hertil.

Ordningen vil således erstatte det gældende system med anmeldelser af behandlinger, der foretages for den offentlige forvaltning, til tilsynsmyndigheden, jf. pkt. 2.6.1.2 nedenfor.

Der henvises i øvrigt til lovforslagets §§ 25 og 26 og bemærkningerne hertil.

2.6. Personoplysningssikkerhed

2.6.1. Gældende ret

2.6.1.1. Persondataloven indeholder i kapitel 11 (§§ 41-42) regler om den fysiske behandlingssikkerhed.

Det fremgår således af lovens § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Efter § 41, stk. 3, skal den dataansvarlige træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Efter persondatalovens § 41, stk. 4, skal der for oplysninger, der behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold (krigsreglen).

Persondatalovens § 41, stk. 5, bemyndiger justitsministeren til at fastsætte nærmere regler om de i stk. 3 anførte sikkerhedsforanstaltninger. Justitsministeren har med hjemmel i bestemmelsen udstedt sikkerhedsbekendtgørelsen og sikkerhedsbekendtgørelsen for domstolene.

Det fremgår af bekendtgørelsernes § 5, at den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af bekendtgørelsen. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinier for

myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.

De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i myndigheden, jf. bestemmelsernes stk. 2.

Bekendtgørelserne indeholder herudover nærmere regler om bl.a. instruktion over for medarbejdere, der behandler personoplysninger, samt om autorisation og adgangskontrol.

Når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker, jf. persondatalovens § 42, stk. 1.

Gennemførelse af en behandling ved en databehandler skal ske i henhold til en skriftlig aftale parterne imellem. Det skal fremgå af aftalen, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren, jf. § 42, stk. 2.

2.6.1.2. Persondatalovens kapitel 12 (§§ 43-47) indeholder regler om anmeldelse af behandlinger, der foretages for den offentlige forvaltning, til Datatilsynet.

Det fremgår således af lovens § 43, jf. § 44, at der skal ske anmeldelse til Datatilsynet forinden iværksættelse af behandling af fortrolige oplysninger. Anmeldelsen skal indeholde en række nærmere angivne oplysninger, herunder om behandlingens formål, en generel beskrivelse af behandlingen, kategorierne af registrerede og foranstaltninger, der iværksættes af hensyn til behandlingssikkerheden og oplysninger om tidspunktet for sletning af oplysningerne.

I visse situationer skal der tillige indhentes en udtalelse fra Datatilsynet, jf. lovens § 45. Der er tale om bl.a. behandlinger, som omfatter følsomme oplysninger eller oplysninger om rent private forhold, og behandlinger, som udelukkende finder sted i videnskabeligt eller statistisk øjemed.

Persondatalovens § 54 indeholder regler om, at Datatilsynet skal føre en fortegnelse over de modtagne anmeldelser, og at denne fortegnelse skal

indeholde de samme oplysninger som anmeldelsen. Den dataansvarlige skal stille disse oplysninger til rådighed for enhver, der anmoder herom, jf. bestemmelsens stk. 2.

2.6.1.3. Persondataloven indeholder ikke regler, hvorefter dataansvarlige, der har sikkerhedsbrud i forbindelse med behandling af personoplysninger, har pligt til at underrette tilsynsmyndigheden herom.

Som nævnt oven for i pkt. 2.3.1.1 indeholder persondatalovens § 5, stk. 1, imidlertid et krav om, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik.

God databehandlingsskik anses efter praksis fra Datatilsynet for bl.a. at omfatte krav til den dataansvarlige om at foretage underretning af berørte personer ved brud på datasikkerheden, når personoplysninger er kommet til uvedkommendes kendskab eller har været i risiko herfor. Ved vurderingen af spørgsmålet om underretning må den dataansvarlige bl.a. tage oplysningernes karakter og de mulige konsekvenser for de berørte i betragtning. Ved utilsigtet offentliggørelse af personoplysninger på en hjemmeside på internettet skal de dataansvarlige således bl.a. foretage underretning af de berørte personer.

Der gælder efter Datatilsynets praksis vedrørende god databehandlingsskik ikke et krav om underretning af *tilsynet* i tilfælde af sikkerhedsbrud.

2.6.2. Retshåndhævelsesdirektivet

2.6.2.1. Direktivets artikel 29 fastsætter detaljerede krav til sikkerheden i forbindelse med behandlingen af personoplysninger.

Efter bestemmelsen forpligtes den dataansvarlige og databehandleren til under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, navnlig for så vidt angår behandlingen af de særlige kategorier af personoplysninger, der er omhandlet i artikel 10.

For så vidt angår automatisk behandling opstilles en række specifikke sikkerhedskrav i bestemmelsen, herunder krav vedrørende kontrol med fysisk

adgang til udstyret, kontrol med datamedier og opbevaring, jf. herved nærmere direktivets artikel 29, stk. 2.

2.6.2.2. Direktivets artikler 30 og 31 indeholder regler om, at den dataansvarlige skal foretage henholdsvis anmeldelse til tilsynsmyndigheden og underretning af den registrerede om brud på datasikkerheden.

Ved brud på persondatasikkerheden skal den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, anmelde bruddet på persondatasikkerheden til tilsynsmyndigheden, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder. Foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen, jf. artikel 30, stk. 1. Databehandleren skal uden unødig forsinkelse underrette den dataansvarlige om brud på persondatasikkerheden, jf. bestemmelsens stk. 2.

Anmeldelsen skal som minimum indeholde en række nærmere angivne oplysninger, herunder om karakteren af bruddet og eventuelle foranstaltninger, som den dataansvarlige har truffet, jf. herved nærmere artikel 30, stk. 2. Hvis bruddet angår oplysninger, der er transmitteret af eller til en dataansvarlig i en anden medlemsstat, skal oplysningerne tillige gives til denne, jf. bestemmelsens stk. 6. Når det ikke er muligt at forelægge alle oplysningerne samlet, kan der ske trinvis forelæggelse, jf. artikel 30, stk. 4.

Direktivets artikel 30, stk. 5, indeholder krav om, at den dataansvarlige skal dokumentere brud på datasikkerheden.

Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal den dataansvarlige uden unødig forsinkelse underrette den registrerede om bruddet på persondatasikkerheden og i den forbindelse give den registrerede en række nærmere angivne oplysninger, herunder om karakteren af bruddet, jf. direktivets artikel 31, stk. 1 og 2.

Det fremgår af direktivets præambelbetragtning nr. 62, at underretninger til registrerede bør gives, så snart det med rimelighed er muligt, i tæt samarbejde med tilsynsmyndigheden og i overensstemmelse med retningslinjer, der er udstukket af denne eller andre relevante myndigheder. Eksempelvis kræver behovet for at begrænse en umiddelbar risiko for skade omgående underretning af de registrerede, mens behovet for at gennemføre

passende foranstaltninger mod fortsatte eller lignende brud på persondatasikkerheden kan begrunde en længere frist for underretningen.

Efter artikel 31, stk. 3, kan underretning af den registrerede i visse tilfælde undlades. Det gælder, når 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.

Der skal heller ikke gives underretning, hvis 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, eller hvis det vil kræve en uforholdsmæssig indsats. I sidstnævnte tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde. Der er efter artikel 31, stk. 5, også mulighed for at udsætte, begrænse eller afskære underretning af de grunde, der er nævnt i direktivets artikel 13, stk. 3, jf. pkt. 2.4.2.1 ovenfor.

Hvis den dataansvarlige ikke allerede har underrettet den registrerede om bruddet på persondatasikkerheden, har tilsynsmyndigheden mulighed for at kræve, at den dataansvarlige foretager underretning, jf. herved nærmere bestemmelsens stk. 4.

2.6.3. Justitsministeriets overvejelser og lovforslagets udformning

2.6.3.1. Direktivets artikel 29 indeholder reglerne om behandlingssikkerhed. Bestemmelsens stk. 1 indeholder det generelle princip om, at de fornødne tekniske og organisatoriske foranstaltninger skal fastsættes ud fra en risikobaseret tilgang, mens bestemmelsens stk. 2 indeholder en detaljeret liste over de konkrete sikkerhedsspørgsmål, som foranstaltningerne skal håndtere, når der er tale om automatisk behandling.

Persondatalovens § 41, stk. 3, og de bekendtgørelser, som er udstedt i medfør af lovens § 41, stk. 5, fastsætter som nævnt oven for i pkt. 2.6.1.1 en række krav til behandlingssikkerheden, som i vidt omfang er sammenfaldende med retshåndhævelsesdirektivets krav.

Det foreslås på den baggrund, at der i overensstemmelse med direktivet fastsættes en regel, som indeholder de nærmere krav til behandlingssikkerheden. Der foreslås endvidere indsat en bemyndigelse til justitsministeren til at fastsætte nærmere regler om disse sikkerhedsforanstaltninger, hvilket vil være en videreførelse af persondatalovens § 41, stk. 5.

Det foreslås endvidere, at den såkaldte krigsregel videreføres med visse modifikationer, jf. nedenfor, hvilket indebærer visse begrænsninger i forhold til anvendelsen af databehandlere fra andre lande, idet en sikring af, at der kan ske bortskaffelse eller tilintetgørelse af oplysningerne i visse automatiske databehandlingssystemer i udgangspunktet forudsætter, at systemerne føres i Danmark. Justitsministeren har tidligere i forbindelse med en besvarelse af spørgsmålene nr. 25, 27, 64 og 69 af 5. januar 1999 fra Folketingets Retsudvalg til lovforslag nr. L 44 af 8. oktober 1998 om behandling af personoplysninger (Folketingstidende 1998-99, tillæg A, s. 943) tilkendegivet, at den gældende krigsregel i persondatalovens § 41, stk. 4, bl.a. indebærer, at Det Centrale Kriminalregister ikke må føres i udlandet.

Spørgsmålet om, hvem der som databehandler kan opbevare oplysninger for en kompetent dansk myndighed, er ikke nærmere reguleret af retshåndhævelsesdirektivet. Et krav om, at et register skal føres i Danmark, kan imidlertid give anledning til at overveje forholdet til EU-rettens almindelige regler om fri bevægelighed, hvor udgangspunktet er, at der ikke må ske forskelsbehandling af databehandlere fra andre medlemsstater.

Det er imidlertid Justitsministeriets vurdering, at kravet i krigsreglen på berettiget vis varetager hensynet til statens sikkerhed, og at kravet derfor under alle omstændigheder er i overensstemmelse med EU-retten, jf. TEUF artikel 52, jf. artikel 65. Hertil kommer, at det følger af retshåndhævelsesdirektivets artikel 2, stk. 3, litra a, at direktivet ikke omfatter behandlinger, som vedrører statens sikkerhed.

I takt med samfundets generelle digitalisering behandler navnlig politiet stadigt stigende mængder oplysninger som led i opgavevaretagelsen. Samtidig indebærer bl.a. hensynet til forsvarerens adgang til at gøre sig bekendt med det materiale, som politiet har indsamlet til brug for en konkret straffesag, at politiet har et stigende behov for at opbevare større mængder oplysninger, herunder personoplysninger. Dette aktualiserer et generelt behov for, at de kompetente myndigheder, i større omfang end det i dag er tilfældet under den gældende regulering, har adgang til at udnytte fleksible

– og sikre – opbevaringsalternativer til den klassiske opbevaring på politiets egne servere.

På den baggrund er der i lovforslaget fundet anledning til at tilpasse den gældende krigsregel, så der i konkrete tilfælde og på baggrund af en nærmere risikovurdering kan gives adgang til, at oplysninger omfattet af krigsreglens anvendelsesområde ikke skal underlægges de i krigsreglen nævnte foranstaltninger, dvs. i praksis en adgang til at opbevare sådanne oplysninger uden for dansk territorium. Dog vil reglen ikke kunne anvendes til at tillade opbevaring uden for EU, idet det findes, at det kun i forhold til de øvrige EU-medlemsstater generelt kan lægges til grund, at oplysninger behandles og beskyttes i overensstemmelse med passende retlige krav mv.

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

2.6.3.2. Direktivets artikel 30 indeholder regler om, at den dataansvarlige skal anmelde brud på datasikkerheden, medmindre det er usandsynligt, at bruddet medfører en risiko for fysiske personers rettigheder.

Der er efter gældende ret ikke noget krav om, at tilsynsmyndigheden skal underrettes ved brud på datasikkerheden.

Det foreslås på den baggrund, at der i overensstemmelse med direktivets artikel 30 fastsættes en regel om, at den dataansvarlige skal underrette tilsynsmyndigheden ved brud på datasikkerheden.

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

2.6.3.3. Direktivets artikel 31 indeholder regler om, at den dataansvarlige skal underrette den registrerede om brud på datasikkerheden, som sandsynligvis vil indebære en høj risiko for den registrerede.

Som nævnt ovenfor i pkt. 2.6.1.3 anses god databehandlingsskik efter persondatalovens § 5, stk. 1, for bl.a. at omfatte krav til den dataansvarlige om at foretage underretning af berørte personer ved brud på datasikkerheden, når personoplysninger er kommet til uvedkommendes kendskab eller har været i risiko herfor.

Direktivets krav om underretning af den registrerede må derfor i vidt omfang anses for at være en videreførelse af gældende ret.

For at sikre, at der ikke kan opstå tvivl om, hvorvidt der er sket korrekt implementering af direktivets artikel 31, foreslås det imidlertid, at der i overensstemmelse med direktivet fastsættes en eksplicit regel om, at den dataansvarlige skal underrette den registrerede om brud på datasikkerheden.

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

2.7. Databeskyttelsesrådgiver

2.7.1. Gældende ret

Der er efter gældende ret ikke nogen forpligtelse for den dataansvarlige til at udpege en databeskyttelsesrådgiver.

2.7.2. Retshåndhævelsesdirektivet

Direktivets artikel 32 indeholder regler om udpegning af en databeskyttelsesrådgiver.

Retshåndhævende myndigheder, der ikke er uafhængige judicielle myndigheder, skal udpege en databeskyttelsesrådgiver på baggrund af dennes faglige kvalifikationer, herunder navnlig inden for databeskyttelsesret, jf. bestemmelsens stk. 1 og 2. Flere myndigheder har mulighed for at udpege en fælles databeskyttelsesrådgiver under hensyntagen til deres organisatoriske struktur og størrelse, jf. stk. 3. Kontaktoplysninger for databeskyttelsesrådgiveren skal offentliggøres og meddeles til tilsynsmyndigheden, jf. bestemmelsens stk. 4.

Efter direktivets artikel 33 skal den dataansvarlige sikre, at databeskyttelsesrådgiveren inddrages i spørgsmål om databeskyttelse og stille de nødvendige ressourcer mv. til rådighed.

Det fremgår af direktivets præambelbetragtning nr. 63, at databeskyttelsesgiveren kan være en af den dataansvarliges eksisterende medarbejdere, som har fået særlig uddannelse inden for databeskyttelsesret og -praksis for at tilegne sig ekspertise på dette område. Vedkommendes opgaver vil kunne udføres på deltid eller fuldtid.

Det fremgår videre af betragtningen, at flere dataansvarlige kan udpege en fælles databeskyttelsesansvarlig i overensstemmelse med deres struktur og

størrelse, for eksempel i tilfælde af fælles ressourcer i centrale enheder. Denne person kan også udpeges til forskellige stillinger i de berørte dataansvarliges struktur.

Det fremgår herudover af betragtningen, at databeskyttelsesrådgivere bør være i stand til at udøve deres opgaver på uafhængig vis i henhold til medlemsstaternes nationale ret.

Direktivets artikel 34 indeholder en liste over de opgaver, som den dataansvarlige som minimum skal overdrage til databeskyttelsesrådgiveren. Der er tale om bl.a. opgaver forbundet med rådgivning af ansatte, overvågning af overholdelsen af reglerne og samarbejde med tilsynsmyndigheden.

2.7.3. Justitsministeriets overvejelser og lovforslagets udformning

Direktivets artikel 32 indeholder regler om udpegelse af en databeskyttelsesrådgiver.

Der følger ikke en forpligtelse til at udpege en databeskyttelsesrådgiver efter gældende ret.

Det foreslås på den baggrund, at der i overensstemmelse med direktivets artikler 32-34 fastsættes regler om, at den dataansvarlige skal udpege en databeskyttelsesrådgiver, og om dennes opgaver.

Det bemærkes i den forbindelse, at de kompetente myndigheder som nævnt i pkt. 2.5.3.3 tillige vil behandle personoplysninger i sager og med formål, som falder uden for det foreslåede anvendelsesområde for loven. Denne behandling vil i stedet være omfattet af persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen. Dette indebærer, at såvel retshåndhævelsesdirektivets som – efter den 25. maj 2018 – databeskyttelsesforordningens krav om udpegelse af en databeskyttelsesrådgiver efter omstændighederne skal være opfyldt.

Forordningens regler om databeskyttelsesrådgiveren adskiller sig på visse punkter fra retshåndhævelsesdirektivets regler herom.

Det er imidlertid Justitsministeriets opfattelse, at de krav til databeskyttelsesrådgiveren, som følger af henholdsvis retshåndhævelsesdirektivet og databeskyttelsesforordningen, ikke strider mod hinanden.

Den person, som udpeges som databeskyttelsesrådgiver, vil således efter retshåndhævelsesdirektivet tillige kunne varetage funktionen som databeskyttelsesrådgiver i medfør af databeskyttelsesforordningen.

Databeskyttelsesrådgiveren vil endvidere kunne fungere som kontaktpunkt, når der er tale om fælles dataansvarlige, jf. pkt. 2.5.3.2.

I forhold til muligheden for, at flere dataansvarlige kan udpege en fælles databeskyttelsesrådgiver, vil dette også være en mulighed på tværs af de kompetente myndigheder, såfremt størrelsen og de organisatoriske forhold tillader dette. Efter Justitsministeriets opfattelse vil en fælles databeskyttelsesrådgiver således kunne udpeges, når flere kompetente myndigheder har tilsvarende organisatoriske opbygninger. Dette vil f.eks. være tilfældet i forhold til de myndigheder, der udgør den overordnede anklagemyndighed. Henset til, at dansk politi udgør et såkaldt enhedspoliti med en fælles ledelse og en homogen organisationsstruktur, vil udpegningen af en fælles databeskyttelsesrådgiver i dansk politi ligeledes være mulig. På tilsvarende måde vil der kunne udpeges en fælles databeskyttelsesrådgiver for samtlige byretter for så vidt angår den behandling af personoplysninger, der foretages, når disse handler uden for deres egenskab af domstole.

I en dansk kontekst varetager de enkelte politikredse både rollen som politi- og anklagemyndighed inden for den samme organisation. Dette vil efter Justitsministeriets opfattelse ikke være til hinder for, at den samme databeskyttelsesrådgiver er udpeget for al den behandling af personoplysninger, som foretages af politikredsen eller som nævnt på tværs af dansk politi.

Der henvises i øvrigt til lovforslagets §§ 30 og 31 og bemærkningerne hertil.

2.8. Overførsler af personoplysninger til tredjelande mv.

2.8.1. Gældende ret

2.8.1.1. Persondatalovens § 27 indeholder regler om overførsel af personoplysninger til tredjelande.

Det fremgår af stk. 1, at der kun må overføres oplysninger til et tredjeland, hvis dette land sikrer et tilstrækkeligt beskyttelsesniveau. Derudover kan der overføres oplysninger til et tredjeland, hvis en af de i stk. 3, nr. 1-8, nævnte betingelser er opfyldt.

Overførsel efter stk. 3 kan bl.a. ske, såfremt overførsel er nødvendig af hensyn til forebyggelse, efterforskning og forfølgning af strafbare forhold samt straffuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig forfølgning eller overførsel er nødvendig af hensyn til den offentlige sikkerhed, rigets forsvar eller statens sikkerhed.

Der kan endvidere ske overførsel, hvis tilsynsmyndigheden har givet særlig tilladelse hertil eller på baggrund af kontrakter, der er i overensstemmelse med standardkontraktbestemmelser, som er godkendt af Europa-Kommissionen, jf. stk. 4 og 5.

Herudover skal persondatalovens almindelige behandlingsregler mv. være opfyldt ved overførsel af oplysninger til tredjelande efter stk. 1 og 3-5, jf. stk. 6.

2.8.1.2. Rammeafgørelsesbekendtgørelsens §§ 4-6 indeholder særlige regler om overførsel til tredjelande eller internationale organer af personoplysninger, som er modtaget fra eller stillet til rådighed af en anden medlemsstat.

Det fremgår af § 4, stk. 1, at videregivelse kun må ske, hvis det er nødvendigt for forebyggelse, efterforskning, afsløring eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner, og den modtagende myndighed i tredjelandet eller det modtagende internationale organ har ansvaret for at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner.

Det kræves endvidere, at den videregivende myndighed i den medlemsstat, som har sendt eller stillet oplysninger til rådighed, har givet sin godkendelse til at videregive disse i henhold til sin nationale lovgivning, og at det pågældende tredjeland eller internationale organ sikrer et tilstrækkeligt beskyttelsesniveau for den påtænkte behandling af oplysningerne.

Der kan dog efter stk. 2 ske videregivelse uden forhåndsgodkendelse fra den videregivende myndighed i den medlemsstat, som har sendt eller stillet oplysninger til rådighed, hvis videregivelsen af oplysningerne er afgørende for forebyggelse af en umiddelbar og alvorlig trussel mod den offentlige sikkerhed i et tredjeland eller et land inden for Den Europæiske Union eller Schengen-samarbejdet, eller videregivelsen af oplysningerne

er afgørende for væsentlige interesser for et land inden for Den Europæiske Union eller Schengen-samarbejdet.

Det er en betingelse for videregivelsen, at forhåndsgodkendelse ikke kan indhentes i tide, og den udenlandske myndighed, der skulle have givet sin godkendelse, skal orienteres omgående.

Der kan efter bestemmelsens stk. 3 ske videregivelse i tilfælde, hvor det pågældende tredjeland eller internationale organ ikke sikrer et tilstrækkeligt beskyttelsesniveau for den påtænkte behandling af oplysningerne, hvis lovgivningen giver mulighed herfor på grund af den registreredes specifikke legitime interesser, eller på grund af legitime vigtige interesser, navnlig vigtige offentlige interesser, eller tredjelandet eller det modtagende internationale organ giver sikkerhedsgarantier, som den videregivende myndighed anser for tilstrækkelige i henhold til sin nationale lovgivning.

2.8.2. Retshåndhævelsesdirektivet

Retshåndhævelsesdirektivets kapitel V fastlægger betingelserne for, hvornår de kompetente myndigheder kan videregive personoplysninger til tredjelande eller internationale organisationer.

Efter direktivets artikel 35, stk. 1, kan overførsel fra en kompetent myndighed til et tredjeland eller til en international organisation, herunder også videreoverførsel til et andet tredjeland eller international organisation, alene finde sted ved opfyldelse af særlige betingelser. Overførslen skal være nødvendig for at opfylde et af de formål, som er omfattet af direktivets anvendelsesområde, og den dataansvarlige i tredjelandet mv. skal være en kompetent myndighed i henhold til disse formål. Hvis personoplysningerne er videregivet eller stillet til rådighed af en anden medlemsstat, skal denne medlemsstat give forudgående tilladelse til overførslen i henhold til dens nationale lovgivning. Oplysninger kan undtagelsesvis overføres uden forudgående tilladelse, hvis det er nødvendigt for at forebygge en umiddelbar og alvorlig trussel mod en medlemsstats eller et tredjelands offentlige sikkerhed eller mod en medlemsstats væsentlige interesser, og den forudgående tilladelse ikke kan indhentes i tide. Den ansvarlige myndighed for den forudgående tilladelse underrettes straks, jf. bestemmelsens stk. 2. Endelig skal Kommissionen have truffet en afgørelse om, at tredjelandet mv. sikrer et tilstrækkeligt beskyttelsesniveau, eller der skal være indført eller eksistere fornødne garantier, jf. direktivets artikler 36 og 37.

I de tilfælde, hvor Kommissionen ikke har truffet en afgørelse om, at tredjelandet mv. sikrer et tilstrækkeligt beskyttelsesniveau, eller der ikke er indført eller eksisterer fornødne garantier, kan overførsel af personoplysninger til et tredjeland mv., kun ske i en række konkrete tilfælde, herunder hvis overførslen er nødvendig for at beskytte den registreredes eller en anden persons vitale interesser, eller hvis overførslen er nødvendig i enkeltsager med henblik på at forfølge de formål, som er omfattet af direktivets anvendelsesområde, jf. herved nærmere direktivets artikel 38.

I individuelle og konkrete sager kan medlemsstaterne endvidere tillade, at der overføres personoplysninger til private i tredjelande, hvis en række betingelser er opfyldt, herunder at overførslen er strengt nødvendig for den overførende myndigheds udførelse af en opgave omfattet af direktivets anvendelsesområde, og at en overførsel til en kompetent myndighed i det pågældende land er ineffektiv eller uhensigtsmæssig, jf. direktivets artikel 39.

2.8.3. Justitsministeriets overvejelser og lovforslagets udformning

Direktivets kapitel V indeholder regler om overførsler af personoplysninger til tredjelande.

Rammeafgørelsen indeholder regler om overførsel af personoplysninger, som er modtaget fra andre medlemsstater; rammeafgørelsen regulerer imidlertid ikke spørgsmålet om overførsel af personoplysninger, som ikke har været udvekslet mellem medlemsstaterne. Sådanne overførsler reguleres derimod i dag af persondataloven.

Med retshåndhævelsesdirektivet introduceres muligheden for at overføre personoplysninger til tredjelande mv. på baggrund af en tilstrækkelighedsafgørelse fra Kommissionen til området for politisamarbejdet og det retlige samarbejde i kriminalsager.

Herudover giver retshåndhævelsesdirektivet mulighed for, at der kan ske overførsel på baggrund af fornødne garantier. Kravet kan opfyldes gennem et retligt bindende instrument eller på baggrund af en konkret vurdering fra den dataansvarlige.

Det foreslås på den baggrund i, at der fastsættes regler, hvorefter der kan ske overførsel af personoplysninger til tredjelande i overensstemmelse med direktivets kapitel V.

Der henvises i øvrigt til lovforslagets §§ 32-36 og bemærkningerne hertil.

2.9. Tilsyn

2.9.1. Gældende ret

2.9.1.1. 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 pkt. 2.9.1.3 nedenfor. Datatilsynet og Domstolsstyrelsen skal samarbejde, i det omfang det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle relevante oplysninger, jf. lovens § 66.

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. lovens §§ 56 og 68, stk. 1, og deres afgørelser kan ikke indbringes for anden administrativ myndighed, jf. §§ 61 og 68, stk. 1, 2. pkt.

Efter § 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.

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. § 62, stk. 2. Tilsvarende gælder for Domstolsstyrelsen, jf. § 68, stk. 1.

Efter lovens §§ 57 og 68, stk. 2, 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 eller – hvis det omhandler domstolenes behandling – Domstolsstyrelsen.

Efter persondatalovens § 65 afgiver Datatilsynet en årlig beretning til Folketinget. Domstolsstyrelsen offentliggør en årlig beretning om dens virksomhed, jf. lovens § 68, stk. 3.

2.9.1.2. Efter lovens § 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.

Lovens § 60, stk. 1, indeholder regler om, hvornår Datatilsynet kan træffe afgørelser over for myndigheder. Af relevans for de myndigheder, som er omfattet af lovforslaget, er afgørelser om overførsler af personoplysninger til tredjelande i medfør af lovens §§ 27, stk. 4, og 58, stk. 2. Med undtagelse af domstolene er der endvidere tale om afgørelser vedrørende den registreredes indsigtsret efter §§ 32, stk. 1, 2 og 4, 33 og 34. For kriminalforsorgen er der tale om afgørelser vedrørende lovens §§ 28-31 om oplysningspligt over for den registrerede, §§ 35 og 37 om den registreredes adgangen til indsigelser, berigtigelse, sletning eller blokering og § 39 om automatiske individuelle afgørelser

I andre tilfælde afgiver tilsynet udtalelser over for den dataansvarlige myndighed, jf. § 60, stk. 2.

Lovens §§ 63, stk. 1, og 68, stk. 1, bemyndiger Datatilsynet henholdsvis Domstolsstyrelsen til at bestemme, at anmeldelser og ansøgninger om tilladelse efter loven og ændringer heri kan eller skal indgives på nærmere angiven måde. Datatilsynet har i medfør af bestemmelsen bl.a. bestemt, at

den offentlige forvaltnings anmeldelse af behandlinger i medfør af reglerne i lovens kapitel 12 skal ske elektronisk via tilsynets hjemmeside.

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

Som nævnt ovenfor i pkt. 2.9.1.1 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.

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, jf. § 67, stk. 3.

2.9.2. Retshåndhævelsesdirektivet

2.9.2.1. Direktivets kapitel VI indeholder regler om oprettelsen af tilsynsmyndigheden og om tilsynsmyndighedens status, opgaver og beføjelser.

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

Direktivets artikel 42 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.

Direktivets artikel 43 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.

Direktivets artikel 44 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 videre af bestemmelsens stk. 2, at medlemmerne skal have tavshedspligt i forhold til de oplysninger, som kommer til deres kendskab under udøvelsen af deres opgaver.

2.9.2.2. Direktivets artikel 45 indeholder regler om tilsynsmyndighedens kompetencer. Det fremgår af bestemmelsens stk. 2, at tilsynsmyndigheden ikke skal have kompetence til at føre tilsyn med domstolenes behandlingsaktiviteter, når de handler i deres egenskab af domstol.

Direktivets artikel 46 indeholder en liste over tilsynsmyndighedens opgaver, herunder 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 pålægges gebyr eller afvises, jf. artikel 46, stk. 4.

Tilsynsmyndigheden skal udarbejde en årlig rapport om sin virksomhed, som skal fremsendes til det nationale parlament og regeringen samt gøres tilgængelig for offentligheden, jf. artikel 49.

2.9.2.3. Direktivets artikel 47 indeholder regler om tilsynsmyndighedens beføjelser, der som minimum skal indeholde beføjelse til at få indsigt i alle de personoplysninger, der behandles, og alle oplysninger, der kræves til udførelse af myndighedens opgaver.

Tilsynsmyndigheden skal herudover have effektive korrigerende beføjelser, f.eks. at udstede advarsler, påbud eller forbud, jf. artikel 47, stk. 2.

Efter direktivets artikel 47, stk. 5, skal tilsynsmyndigheden have beføjelser til at indbringe overtrædelser af de bestemmelser, der vedtages i henhold til direktivet, for de judicielle myndigheder og om nødvendigt at indlede eller på anden måde deltage i retssager med henblik på at håndhæve disse bestemmelser.

Det fremgår af direktivets præambelbetragtning nr. 82, at tilsynsmyndighedernes beføjelser ikke bør gribe ind i de særlige regler for straffesager,

herunder efterforskning og retsforfølgning af strafbare handlinger, eller i retsvæsnets uafhængighed.

2.9.2.4. Tilsynsmyndighederne skal efter direktivets artikel 50 samarbejde såvel nationalt som medlemsstaterne i mellem. Bestemmelsens stk. 2-7 indeholder nærmere regler om samarbejdet mellem tilsynsmyndighederne i forskellige medlemsstater, herunder regler om, at anmodninger skal besvares uden unødig 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 direktivet eller med EU-ret eller national ret, som den modtagende tilsynsmyndigheder er underlagt.

2.9.3. Justitsministeriets overvejelser og lovforslagets udformning

Direktivets kapitel VI indeholder regler om oprettelsen af tilsynsmyndigheden og om tilsynsmyndighedens status, opgaver og beføjelser. Reglerne er sammenfaldende med reglerne om tilsynsmyndigheden i databeskyttelsesforordningens kapitel VI.

2.9.3.1. I forhold til Datatilsynets organisation foreslås der i vidt omfang en videreførelse af den gældende ordning.

Det er imidlertid et krav efter direktivets artikel 44, stk. 1, litra e, at medlemsstaterne fastsætter regler om, hvorvidt der ske genudnævnelse af medlemmer af tilsynsmyndigheden, og i givet fald hvor mange gange, at der kan ske genudnævnelse.

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

Justitsministeriet finder desuden, at karakteren af de oplysninger om de kompetente myndigheder automatiske databehandlingssystemer, som vil kunne tilgå rådet, kan begrunde, at der fremover stilles krav om, at rådets formand, medlemmer og stedfortrædende medlemmer kan sikkerhedsgodkendes, og at sikkerhedsgodkendelsen kan opretholdes i hele embedsperioden. En sådan ordning er i overensstemmelse med direktivets artikel 43, stk. 4, hvorefter et medlem bl.a. kan afskediges, hvis den pågældende ikke længere opfylder betingelserne for at varetage sit hverv.

I forhold til direktivets 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 44, stk. 2, er det Justitsministeriets vurdering, at dette krav er opfyldt gennem Datarådets forretningsorden, jf. pkt. 2.9.1.1 ovenfor, forvaltningslovens § 27 og straffelovens § 152.

Der henvises i øvrigt til lovforslagets § 37 og bemærkningerne hertil.

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

Der foreslås 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.

Der henvises i øvrigt til lovforslagets § 38 og bemærkningerne hertil.

2.9.3.3. For så vidt angår spørgsmålet om tilsynsmyndighedernes uafhængighed, som er reguleret i direktivets artikel 42, 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 §§ 55-56 og §§ 67-68 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 § 56 i den danske persondatalov 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 videre af besvarelsen, at det af forarbejderne til persondataloven (Folketingstidende 1999-2000, tillæg A, s. 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.

Det foreslås på den baggrund, at der fastsættes regler om, at tilsynsmyndigheden skal udøve sine funktioner i fuld uafhængighed. Den foreslåede bestemmelse omfatter således tillige de aspekter af uafhængighedskravet, som er anført i direktivets artikel 42, stk. 2-6. I forhold til spørgsmålet om tilsynsmyndighedens budget, som efter direktivets artikel 42, 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 § 39 og bemærkningerne hertil.

2.10. Retsmidler, ansvar og sanktioner

2.10.1. Gældende ret

Bestemmelser om erstatning- og strafansvar er fastsat i persondatalovens kapitel 18 (§§ 69-71). Den generelle adgang til at klage til tilsynsmyndigheden over behandling af personoplysninger findes i lovens § 40.

2.10.1.1. 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 dansk rets almindelige erstatningsretlige regler.

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

2.10.1.2. Lovens § 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 tredjemand i statistisk eller videnskabeligt øjemed), § 13, stk. 1 (om registrering af udgående telefonopkald), § 27, stk. 4 (overførsel af oplysninger til tredjelande), 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.

2.10.2. Retshåndhævelsesdirektivet

2.10.2.1. Efter direktivets artikel 52 skal enhver registreret have adgang til at indgive klager til tilsynsmyndigheden. Sendes klagen til den forkerte tilsynsmyndighed, skal der ske videresendelse. Tilsynsmyndigheden skal efter anmodning yde bistand til den registrerede og skal underrette den pågældende om forløbet og resultatet af klagen samt vejlede om adgangen til retsmidler.

2.10.2.2. Efter direktivets artikler 53 og 54 skal den registrerede – med forbehold af en eventuel administrativ klageadgang – have ret til at indbringe henholdsvis tilsynsmyndighedens afgørelser og spørgsmål om dataansvarliges og databehandleres krænkelser af de rettigheder, der garanteres vedkommende i henhold til national lovgivning, for en domstol. En sag mod en tilsynsmyndighed skal anlægges i den medlemsstat, hvor tilsynsmyndigheden er etableret, jf. artikel 53 stk. 3.

2.10.2.3. Den registrerede skal i overensstemmelse med nationale retsplejeregler have ret til at bemyndige 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, til at indgive en klage på sine vegne og til at udøve de rettigheder, der er omhandlet i artikel 52, 53 og 54 på sine vegne.

Det fremgår af direktivets præambelbetragtning nr. 87, at den registreredes ret til at lade sig repræsentere ikke bør berøre medlemsstaternes nationale retsplejeregler, som vil kunne kræve obligatorisk repræsentation af registrerede ved advokat for en national domstol.

2.10.2.4. Direktivets artikel 56 omhandler retten til erstatning. Efter bestemmelsen er enhver, der har lidt skade som følge af en ulovlig handling eller enhver anden handling, der er uforenelig med de nationale bestemmelser, der vedtages til gennemførelse af direktivet, berettiget til erstatning for den forvoldte skade fra den kompetente myndighed (eller en anden myndighed, der er kompetent i henhold til den nationale lovgivning).

2.10.2.5. Efter artikel 57 fastsætter medlemsstaterne regler om sanktioner, der er effektive, står i et rimeligt forhold til lovovertrædelsen, har afskrækkende virkning, og som skal finde anvendelse i tilfælde af overtrædelse af de bestemmelser, der vedtages til gennemførelse af direktivet.

2.10.3. Justitsministeriets overvejelser og lovforslagets udformning

2.10.3.1. Direktivets artikel 52 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 § 48, stk. 1, og bemærkningerne hertil.

2.10.3.2. Direktivets artikel 53 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 direktivet 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 havde 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 tilsynsmyndigheders 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 § 48, stk. 2, og bemærkningerne hertil.

2.10.3.3. Efter direktivets artikel 54 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 pkt. 2.10.3.2 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 databehandleres 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 § 48, stk. 2 og 3, og bemærkningerne hertil.

2.10.3.4. Efter direktivets artikel 55 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 direktivet 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 direktivets artikel 55.

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 sige 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 man-

datarer. 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.

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 § 48 og bemærkningerne hertil.

2.10.3.5. Det fremgår af direktivets artikel 56, at enhver, som har lidt materiel eller immateriel skade som følge af en ulovlig behandlingsaktivitet eller en overtrædelse af de nationale regler, der vedtages i henhold til direktivet, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller en anden myndighed, der er kompetent i henhold til national ret.

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, s. 4043 f.), at valget af præsumptionsansvar som ansvarsgrundlag var påkrævet for at sikre en korrekt implementering af databeskyttelsesdirektivet.

Retshåndhævelsesdirektivets artikel 56 regulerer i modsætning til databeskyttelsesdirektivet ikke nærmere, hvordan reglerne om erstatning skal udformes, herunder hvilket ansvarsgrundlag der skal anvendes. Der må derfor antages at være et vist råderum for medlemsstaterne på dette punkt.

Det er Justitsministeriets opfattelse, at spørgsmål om erstatning for overtrædelse af lovens bestemmelser skal håndteres i medfør af de almindelige erstatningsretlige regler i dansk ret, og at der ikke er grundlag eller behov for at fastsætte et skærpet præsumptionsansvar. De registreredes muligheder for at godtgøre, at der foreligger et erstatningsansvar, skal således ses i lyset af de registreredes adgang til at klage til tilsynsmyndighederne med den deraf følgende adgang til at anvende tilsynsmyndighedernes afgørelser i en efterfølgende erstatningssag. Hertil kommer, at det ikke er et krav efter retshåndhævelsesdirektivet, at der fastsættes et skærpet præsumptionsansvar.

Justitsministeriet finder således, at adgangen til erstatning skal følge de almindelige erstatningsretlige principper i dansk ret.

Retshåndhævelsesdirektivets artikel 56 drejer sig om adgangen til at søge erstatning hos den dataansvarlige for skade som følge af en ulovlig behandlingsaktivitet eller enhver anden behandling i strid med de nationale regler, som gennemfører direktivet. For så vidt angår de tilfælde, hvor skaden er opstået som følge af en culpøs handling eller undladelse foretaget af en databehandler, vil den dataansvarlige efter omstændighederne kunne gøre et regreskrav gældende mod databehandleren. Adgangen hertil reguleres ikke af retshåndhævelsesdirektivet, men vil kunne være reguleret af databehandleraftalen, og vil i øvrigt afhænge af, om der foreligger et ansvarsgrundlag efter de almindelige regler om erstatning inden for kontraktforhold.

Der henvises i øvrigt til lovforslagets § 49 og bemærkningerne hertil.

2.10.3.6. Direktivets artikel 57 forpligter medlemsstaterne til at fastsætte regler om sanktioner, samt at træffe alle nødvendige foranstaltninger for at sikre, at sanktionerne anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Persondatalovens § 70, stk. 2, indeholder regler om straf i forbindelse med behandling, som udføres for offentlige myndigheder. Handlinger, der tilli-

ge 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 m.v., herunder bl.a. §§ 152 og 152 c-f samt §§ 155-157.

Strafansvar efter persondatalovens § 70, stk. 2, vedrører primært bestemmelser, som private databehandlere, der udfører opgaver for offentlige myndigheder, skal iagttage. Strafansvar i forhold til den offentlige myndighed er navnlig relevant ved overtrædelser af vilkår fastsat af Datatilsynet. Offentlige myndigheder kan ifalde strafansvar for overtrædelse af persondataloven i overensstemmelse med straffelovens regler om strafansvar for juridiske personer mv.

Det foreslås på den baggrund, at der fastsættes en bestemmelse, hvor private dataansvarlige kan ifalde strafansvar i forhold til behandling, som udføres for de kompetente myndigheder, og hvor de kompetente myndigheder kan ifalde strafansvar ved overtrædelse af påbud og forbud, der er meddelt i henhold til den foreslåede § 42.

Med den foreslåede ordning sikres det, at tilsynsmyndighederne har en reaktionsmulighed i tilfælde af, at en kompetent myndighed ikke overholder et påbud eller forbud.

Strafansvaret efter denne bestemmelse vil således navnlig være relevant i forhold til overtrædelser af generel eller systematisk karakter, idet strafansvar for så vidt angår overtrædelser i form af konkrete behandlinger, f.eks. en polititjenestemands uberettigede videregivelse af personoplysninger til et nyhedsmedie, som typisk ikke vil blive genstand for påbud eller forbud fra tilsynsmyndigheder, fortsat vil kunne fastlægges i medfør af straffelovens regler suppleret af eventuelle disciplinære reaktioner.

Strafansvaret for offentlige myndigheder skal også fortsat pålægges i overensstemmelse med reglerne i straffelovens 5. kapitel, herunder straffelovens § 27, stk. 2. Det følger heraf, 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 i øvrigt til lovforslagets § 50 og bemærkningerne hertil.

3. Økonomiske og administrative konsekvenser for det offentlige

Der udstår en vurdering af lovforslagets økonomiske og administrative konsekvenser for det offentlige.

4. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ikke administrative eller økonomiske konsekvenser for erhvervslivet.

5. Administrative konsekvenser for borgerne

6. Miljømæssige konsekvenser

Lovforslaget har ikke miljømæssige konsekvenser.

7. Forholdet til EU-retten

Lovforslaget gennemfører Europa-Parlamentets og Rådets direktiv 2016/680/EU 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.

8. Hørte myndigheder og organisationer mv.

Et udkast til lovforslaget har i perioden fra den 1. marts 2017 til den 15. marts 2017 været sendt i høring hos følgende myndigheder og organisationer mv.:

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	Ingen	Ingen
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget gennemfører Europa-Parlamentets og Rådets direktiv 2016/680/EU 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.	
Overimplementering af EU-retlige minimumsforpligtelser (sæt X)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Til stk. 1

Persondataloven gælder generelt for behandling af personoplysninger, der 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, jf. lovens § 1, stk. 1. Regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i persondataloven, jf. § 2, stk. 1.

Persondataloven gælder således også for politiets, militærpolitiets, anklagemyndighedens, herunder den militære anklagemyndigheds, kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger.

Det fremgår imidlertid af lovens § 2, stk. 4, at lovens bestemmelser om oplysningspligt over for den registrerede (kapitel 8), den registreredes ret til indsigelse, berigtigelse, blokering og sletning af personoplysninger (§§ 35-37) og om automatiske afgørelser (§ 39) ikke finder anvendelse på behandlinger, der foretages for domstolene, politiet og anklagemyndigheden inden for det strafferetlige område. Herudover finder lovens regler om den registreredes ret til indsigt (kapitel 9) ikke anvendelse på behandlinger, der foretages for domstolene inden for det strafferetlige område.

Det foreslås i *§ 1, stk. 1*, at loven skal gælde for politiets, militærpolitiets, anklagemyndighedens, herunder den militære anklagemyndigheds, Den Uafhængige Politiklagemyndigheds, kriminalforsorgens og domstolenes 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, når behandlingen foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

Efter den foreslåede ordning er lovens anvendelsesområde begrænset til de kompetente myndigheders behandling af personoplysninger med henblik på at *forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler med den offentlige sikkerhed*.

Loven finder således først og fremmest anvendelse på den behandling af personoplysninger, som finder sted i forbindelse med de kompetente myndigheders aktiviteter inden for strafferetsplejen.

For så vidt angår udstrækningen af begrebet *forebyggelse* af strafbare handlinger vil dette omfatte de aktiviteter, der udøves som led i de kompetente myndigheders generelle og individualiserede forebyggelsesindsatser, f.eks. indsatsen for at understøtte personers exit fra rocker- og bandemiljøet, lokalpolitiets kriminalitetsforebyggende arbejde, indsatsen mod radikalisering, bekymringssamtaler med udsatte unge og lignende. Anvendelsesområdet knytter sig således også til generelle forebyggelsesindsatser, f.eks. i forhold til de dele af færdselskontrolindsatsen, som ikke – endnu – har forbindelse til konkrete strafbare forhold.

Indsamling og behandling af personoplysninger, der er knyttet til *efterforskningen* og *afsløringen* af en konkret strafbar handling, såvel som politiets mere generelle monitorering af kriminalitetsområder, kriminelle miljøer mv. på såvel taktisk som strategisk plan, er ligeledes omfattet af det foreslåede anvendelsesområde.

For så vidt angår *retsforfølgningen* af strafbare handlinger, vil samtlige behandlinger af personoplysninger, der finder sted som led i politiets og anklagemyndighedens forberedelse og gennemførelse af straffesager, være omfattet af anvendelsesområdet. Behandlingen af personoplysninger om sigtede, tiltalte, vidner, domsmænd mv. i den forbindelse, vil således i det hele være omfattet.

Endelig vil de kompetente myndigheders behandling af personoplysninger med henblik på opgaver knyttet til *fuldbyrdelse* af strafferetlige sanktioner falde ind under anvendelsesområdet.

Loven vil endvidere finde anvendelse på aktiviteter, som ikke er knyttet til en helt konkret strafbar handling, f.eks. udøvelsen af beføjelser gennem *tvangsindgreb* som f.eks. politiaktiviteter i forbindelse med demonstrationer, store sportsbegivenheder og uroligheder.

Disse aktiviteter omfatter også opretholdelse af lov og orden som en opgave, der er overdraget til politiet eller andre retshåndhævende myndigheder, hvor det er nødvendigt for at *beskytte mod og forebygge trusler mod den offentlige sikkerhed* og de ved lov beskyttede grundlæggende samfundsinteresser, *som kan føre til en strafbar handling*.

Uden for lovens anvendelsesområde falder de administrative sager, som behandles af de kompetente myndigheder, herunder politiets behandling af klager over politiets dispositioner inden for og udenfor strafferetsplejen, udstedelse af tilladelser til udøvelse af forskellige hverv, herunder pantelånere, idrætskontrollører, dørmænd og vagter, samt tilladelser til afholdelse af forskellige offentlige arrangementer eller aktiviteter, herunder forlystelser, boksekampe og særtransporter. Ligeledes modtager og behandler politiet og andre retshåndhævende myndigheder, som andre forvaltningsmyndigheder, løbende aktindsigtsanmodninger efter offentlighedsloven og forvaltningsloven og vil også fremadrettet skulle behandle personoplysninger i forbindelse med behandlingen af konkrete anmodninger om indsigt i henhold til den gældende databeskyttelsesretlige regulering.

På tilsvarende måde vil behandling af personoplysninger, der finder sted i forbindelse med de kompetente myndigheders ansættelse af medarbejdere og den løbende administration af ansættelsesmæssige forhold falde uden for lovens anvendelsesområde.

Behandling af personoplysninger i sådanne sager vil i stedet være omfattet af de generelle regler i persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen.

Der henvises i øvrigt til pkt. 2.1.3 i lovforslagets almindelige bemærkninger.

Til stk. 2

Det fremgår af persondatalovens § 2, stk. 1, at loven ikke gælder for den behandling, der udføres for politiets og forsvarets efterretningstjenester. Rammeafgørelsesbekendtgørelsens § 1, stk. 3, indeholder en tilsvarende bestemmelse.

Den foreslåede *§ 1, stk. 2*, viderefører den gældende ordning vedrørende efterretningstjenesterne. Under bestemmelsen falder også den behandling af personoplysninger, som foretages af den militære anklagemyndighed i forbindelse med sager vedrørende ansatte i Forsvarets Efterretningstjeneste.

Der henvises i øvrigt til pkt. 2.1.3.6 i lovforslagets almindelige bemærkninger.

Til stk. 3

Det fremgår af rammeafgørelsesbekendtgørelsens § 1, stk. 1, at bekendtgørelsen ikke finder anvendelse i forhold til personoplysninger, der udveksles eller stilles til rådighed i forbindelse med samarbejde efter Rådets afgørelse 2008/615/RIA af 23. juni 2008 om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet (Prümafgørelsen), eller efter Konvention om gensidig retshjælp i straffesager mellem den Den Europæiske Unions medlemsstater.

Det foreslås i *§ 1, stk. 3,* at loven ikke skal finde anvendelse i forhold til behandling af personoplysninger i medfør af EU-retsakter, der den eller inden den 6. maj 2016 er trådt i kraft på området for retligt samarbejde i straffesager og politisamarbejde, og som regulerer behandling mellem medlemsstaterne og medlemsstaternes udpegede myndigheders adgang til EU-informationssystemer.

Den foreslåede ordning indebærer, at de regler om behandling af personoplysninger i gældende EU-retsakter – eller nationale regler, der implementerer sådanne EU-retsakter – fortsat finder anvendelse. Det gælder f.eks. de kompetente myndigheders udveksling af oplysninger om f.eks. DNA og fingeraftryk i medfør af Prüm-afgørelsen, jf. ovenfor

Til § 2

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

Det fremgår af forarbejderne til persondataloven (Folketingstidende 1999-2000, tillæg A, s. 4057), at persondataloven finder anvendelse, hvis regler om behandling af personoplysninger i anden lovgivning giver den registrerede en dårlige retsstilling. Dette gælder dog ikke, hvis den dårlige retsstilling har været tilsigtet og i øvrigt ikke strider mod reglerne i databeskyttelsesdirektivet.

Det foreslås i *§ 2* at videreføre den gældende bestemmelse i persondatalovens § 2.

Efter den foreslåede bestemmelse vil lovforslaget således ikke finde anvendelse, hvis den registrerede opnår en bedre retsstilling efter anden lovgivning. Anden lovgivning, som giver den registrerede en dårlige retsstilling, finder dog anvendelse, hvis den dårlige retsstilling har været tilsigtet og i øvrigt ikke strider mod reglerne i retshåndhævelsesdirektivet. Bestemmelsen indebærer ikke, at databeskyttelsesforordningens regler vil finde anvendelse, desuagtet at denne i en konkret sammenhæng kan siges at føre til en bedre retsstilling for den registrerede. Den foreslåede bestemmelse vil således alene finde anvendelse i forhold til bestemmelser, der regulerer de kompetente myndigheders behandling af personoplysninger inden for lovens anvendelsesområde. Som eksempel på sådanne bestemmelser kan der peges på bestemmelserne i retsplejelovens §§ 818 og 819, der bl.a. regulerer behandlingen af personoplysninger i forbindelse med politiets udstedelse af signalementer og efterlysninger. Disse bestemmelser fastsætter særlige bestemmelser, der efter omstændighederne giver den registrerede en bedre retsstilling.

Der henvises i øvrigt til pkt. 2.1.3.7 i lovforslagets almindelige bemærkninger.

Til § 3

Til nr. 1

Det fremgår af persondatalovens § 3, nr. 1, at personoplysninger defineres som enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).

Det foreslås i *§ 3, nr. 1*, at personoplysninger defineres som 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 online-identifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet, jf. herved retshåndhævelsesdirektivets artikel 3, nr. 1.

Der er således tale om en videreførelse af definitionen af personoplysninger i persondataloven.

Til nr. 2

Det fremgår af persondatalovens § 3, nr. 2, at behandling defineres som enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.

Det foreslås i *§ 3, nr. 2*, at behandling defineres som enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for.

Behandling omfatter således f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, overførsel til tredjeland, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse, jf. herved retshåndhævelsesdirektivets artikel 3, nr. 2.

Der er således i praksis tale om en videreførelse af definitionen af behandling i persondataloven.

Til nr. 3

Persondataloven indeholder ikke en definition af begrebet begrænsning af behandling.

Det fremgår imidlertid af persondatalovens § 37, stk. 1, at den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Det fremgår af forarbejderne til persondataloven (Folketingstidende 1999-2000, tillæg A, s. 4092), at blokering af oplysninger indebærer, at det fortsat er tilladt at opbevare indsamlede oplysninger, hvorimod det ikke er tilladt at behandle og bruge oplysninger, herunder navnlig videregive dem til tredjemand. Oplysninger, som er blokeret, skal derfor være forsynet med en sådan markering, at en bruger informeres om blokeringen.

Det foreslås i *§ 3, nr. 3*, at begrænsning af behandling defineres som mærkning af opbevarede personoplysninger med den hensigt at begrænse fremtidig behandling af disse oplysninger.

Begrænsning kan ske ved, at udvalgte oplysninger flyttes til et andet behandlingssystem, f.eks. til arkivformål, eller at udvalgte oplysninger gøres utilgængelige. I automatiske registre kan begrænsning ske ved hjælp af tekniske hjælpemidler. En begrænsning skal anføres i registeret på sådan måde, at det tydeligt fremgår, at behandlingen af personoplysninger er begrænset, jf. herved direktivets præambelbetragtning nr. 47.

Der er således i praksis tale om en videreførelse af den forståelse af begrebet blokering, som følger af persondataloven.

Til nr. 4

Persondataloven indeholder ikke en definition af begrebet profilering.

Det foreslås i *§ 3, nr. 4*, at profilering defineres som enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person.

Profilering kan navnlig have til formål at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser, jf. retshåndhævelsesdirektivets artikel 3, nr. 4.

Til nr. 5

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

Det foreslås i *§ 3, nr. 5*, at register defineres som enhver struktureret samling af personoplysninger, der er tilgængelig efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på funktionsbestemt eller geografisk grundlag.

Der er således tale om en videreførelse af definitionen af register i persondataloven.

Til nr. 6

Persondataloven indeholder ikke en definition af kompetente myndigheder.

Det foreslås i *§ 3, nr. 6*, at kompetente myndigheder defineres som enhver offentlig myndighed eller ethvert andet organ eller enhver anden enhed, der i henhold til medlemsstaternes nationale ret er bemyndiget med hensyn til at udøve offentlig myndighed og offentlige beføjelser med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

Det foreslås endvidere, at det i definitionen præciseres, at de kompetente myndigheder i Danmark er politiet, militærpolitiet, anklagemyndigheden, herunder den militære anklagemyndighed, kriminalforsorgen, Den Uafhængige Politiklagemyndighed og domstolene.

Den generelle definition er relevant i forbindelse med den udveksling af oplysninger, der sker mellem de danske kompetente myndigheder og de kompetente myndigheder i andre medlemsstater.

Til nr. 7

Det fremgår af persondatalovens § 3, nr. 4, at begrebet den dataansvarlige defineres som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger.

Det foreslås i *§ 3, nr. 7*, at begrebet den dataansvarlige defineres som den kompetente myndighed, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Definitionen er således knyttet til definitionen af de kompetente myndigheder, da det alene er disse myndigheders behandling af personoplysninger, der er omfattet af det foreslåede anvendelsesområde for loven.

Til nr. 8

Det fremgår af persondatalovens § 3, nr. 5, at begrebet databehandleren defineres som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.

Det foreslås i *§ 3, nr. 8*, at begrebet databehandleren defineres som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.

Der er således tale om en videreførelse af definitionen af databehandler i persondataloven.

Til nr. 9

Det fremgår af persondatalovens § 3, nr. 7, at begrebet modtager defineres som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, hvortil oplysningerne meddeles, uanset om der er tale om en tredjemand. Myndigheder, som vil kunne få meddelt oplysninger som led i en isoleret forespørgsel, betragtes ikke som modtagere.

Det foreslås i *§ 3, nr. 9*, at begrebet modtager defineres som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, hvortil personoplysninger videregives, således at modtageren selvstændigt herefter træffer beslutning om, til hvilket formål og med hvilke midler denne behandler de videregivne oplysninger, uanset om det er en tredjemand eller ej. Myndigheder, som vil kunne få meddelt personoplysninger som led i en isoleret forespørgsel, betragtes ikke som modtagere.

Angivelsen af, at myndigheder, som vil kunne få meddelt personoplysninger som led i en isoleret forespørgsel, ikke betragtes som modtagere, er relevant i forhold til de myndigheder, som de kompetente myndigheder løbende samarbejder med f.eks. i forbindelse med konkrete efterforskninger af strafbare forhold. I det omfang der i den forbindelse – inden for gældende ret i øvrigt – finder enkeltstående videregivelser af personoplys-

ninger sted, vil den eller de modtagende myndigheder ikke være at anse som modtagere i bestemmelsens forstand. Eksempler på myndigheder, der i overensstemmelse med gældende ret kan få personoplysninger meddelt som led i en isoleret forespørgsel omfatter bl.a. skattemyndighederne, Finanstilsynet og andre myndigheder, der på lignende vis udøver tilsyns- og kontrolbeføjelser. Dette vil bl.a. have betydning for, hvilke oplysninger der skal meddeles i forbindelse med iagttagelsen af lovens regler om oplysninger, der skal stilles til rådighed for eller gives til den registrerede, jf. § 13, stk. 2.

Videregivelse til myndigheder, der efter gældende ret skal finde sted i mere systematisk omfang, eller uden at der foretages en konkret vurdering af, om videregivelsen skal finde sted, vil ikke være at anse som isoleret i bestemmelsens forstand. Ligeledes vil en videregivelse af et register som helhed eller en videregivelse med henblik på at gennemføre en samkøring af registre ikke udgøre en enkeltstående videregivelse som led i en isoleret forespørgsel.

Til nr. 10

Persondataloven indeholder ikke en definition af begrebet brud på persondatasikkerheden.

Det foreslås i *§ 3, nr. 10*, at brud på persondatasikkerheden defineres som ethvert 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, jf. direktivets artikel 3, nr. 11.

Til nr. 11

Persondataloven indeholder ikke en definition af begrebet genetiske data.

Det foreslås i *§ 3, nr. 11*, at begrebet genetiske data defineres som 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.

Den biologiske prøve kan f.eks. være en analyse på kromosomniveau, af deoxyribonukleinsyre (DNA) eller ribonukleinsyre (RNA), eller efter en

analyse af et andet element til indhentning af lignende oplysninger, jf. retshåndhævelsesdirektivets præambelbetragtning nr. 23.

Til nr. 12

Persondataloven indeholder ikke en definition af begrebet biometriske data.

Det foreslås i *§ 3, nr. 12*, at begrebet biometriske data defineres som 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.

Til nr. 13

Persondataloven indeholder ikke en definition af begrebet helbredsoplysninger.

Det foreslås i *§ 3, nr. 12*, at begrebet helbredsoplysninger defineres som personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand.

Helbredsoplysninger omfatter alle personoplysninger om den registreredes helbredstilstand, som giver oplysninger om den registreredes tidligere, nuværende eller fremtidige fysiske eller mentale helbredstilstand, dvs. enhver oplysninger 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 prøveudtagningsudstyr.

Der kan endvidere være tale om oplysninger, der hidrører fra prøver eller undersøgelser af en legemsdel eller legemlig substans, herunder fra genetiske data og biologiske prøver.

Til nr. 14

Persondataloven indeholder ikke en definition af begrebet international organisation.

Det foreslås i *§ 3, nr. 14*, at begrebet international organisation defineres som en folkeretlig organisation og organer, der er underordnet en sådan organisation, samt ethvert andet organ, der er oprettet ved eller med hjemmel i en aftale mellem to eller flere lande.

Omfattet af definitionen er f.eks. Interpol, som Danmark og de øvrige EU-medlemsstater er tilknyttet.

Til § 4

Til stk. 1.

Det fremgår af persondatalovens § 5, stk. 1, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik.

God databehandlingsskik er en retlig standard, som udfyldes af tilsynsmyndighederne. Begrebet indebærer bl.a., at behandlingen af oplysninger skal være rimelig og lovlig.

God databehandlingsskik anses efter praksis fra Datatilsynet for bl.a. at omfatte krav til den dataansvarlige om forudgående underretning af den registrerede om visse behandlingsaktiviteter, en pligt til at notere den registreredes indsigelser i forhold til rigtigheden af de registrerede oplysninger og underretning af berørte personer ved brud på datasikkerheden. God databehandlingsskik supplerer således navnlig lovens regler om den registreredes rettigheder.

Det foreslås i *§ 4, stk. 1*, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik og under hensyntagen til oplysningernes karakter.

Der sker således en videreførelse af begrebet god databehandlingsskik. Dette indebærer, at behandling skal være lovlig, rimelig og gennemsigtig i forhold til de registrerede, samt at der – på samme måde som i dag – vil være tale om en retlig standard, som skal udfyldes af tilsynsmyndighederne.

Kravet forhindrer ikke i sig selv de kompetente myndigheder i at udføre aktiviteter som f.eks. hemmelige undersøgelser eller videoovervågning, så

længe dette sker under behørig hensyntagen til de berørte registreredes legitime interesser.

Kravet om, at der skal tages hensyn til oplysningernes karakter, indebærer, at der skal sondres mellem personoplysninger, der bygger på faktiske omstændigheder, og personoplysninger, der bygger på personlige vurderinger, jf. herved retshåndhævelsesdirektivets artikel 7, stk. 1.

Dette har f.eks. betydning i forhold til vurderingen af oplysningernes rigtighed. Navnlig i retssager er udsagn, der indeholder personoplysninger, baseret på en subjektiv opfattelse af fysiske personer, og det er ikke altid muligt at kontrollere dem. Kravet om oplysningernes rigtighed bør derfor ikke vedrøre et udsagns rigtighed, men blot det forhold, at der er fremsat et konkret udsagn.

Der henvises i øvrigt til pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 2

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

Det fremgår af lovens forarbejder (Folketingstidende 1999-2000, tillæg A, s. 4064), at der i kravet om udtrykkelighed ligger, at den dataansvarlige i forbindelse med indsamlingen skal angive et formål, som er tilstrækkeligt veldefineret og velafgrænset til at skabe åbenhed og klarhed omkring behandlingen. Formålet med behandlingen af oplysningerne skal således defineres med en vis præcision. Der henvises i den forbindelse til, at en formålsangivelse som f.eks. ”til brug for udbud af finansielle ydelser” anses for at være tilstrækkelig præcis.

Det foreslås i *§ 4, stk. 2*, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, som er omfattet af den foreslåede § 1, og senere behandling må ikke være uforenelig med disse formål, idet der dog henvises til den forslåede § 5, som angiver betingelserne for, hvornår en efterfølgende behandling kan finde sted. Der er i vidt omfang tale om en videreførelse af gældende ret.

Adgangen til at behandle oplysninger i historisk, statistisk eller videnskabeligt øjemed er således delvist reguleret i den foreslåede § 5 for så vidt, at der er tale om en behandling med et formål, som er omfattet af lovens anvendelsesområde. Såfremt formålet falder uden for lovens anvendelsesområde – hvilket i praksis ofte vil være tilfældet – vil behandlingen skulle ske på baggrund af persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen.

Der henvises i øvrigt til pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 3

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

Det foreslås i *§ 4, stk. 3*, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere end der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Der er således tale om en videreførelse af gældende ret.

Der henvises i øvrigt til pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 4

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

Det foreslås i *§ 4, stk. 4*, at oplysninger, som behandles, skal være korrekte og om nødvendigt ajourførte, og at 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.

Der er således tale om en videreførelse af gældende ret. De sproglige forskelle mellem persondatalovens § 5, stk. 4, og den foreslåede § 5, stk. 4, skyldes således alene hensynet til at sikre, at der ikke kan opstå tvivl om, hvorvidt der er sket en korrekt gennemførelse af retshåndhævelsesdirektivets artikel 4, stk. 1, litra c.

Der henvises i øvrigt til pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 5

Det fremgår af persondatalovens § 5, stk. 4, 2. pkt., at der skal foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger.

Det fremgår af rammeafgørelsesbekendtgørelsens § 9, stk. 1, at den dataansvarlige skal træffe alle rimelige foranstaltninger til at sikre, at personoplysninger ikke videregives eller stilles til rådighed, hvis de er urigtige, ufuldstændige eller ikke ajourførte. I dette øjemed verificerer den dataansvarlige så vidt muligt kvaliteten af personoplysningerne, før de videregives eller stilles til rådighed. I forbindelse med al videregivelse af oplysninger skal der så vidt muligt tilføjes tilgængelige oplysninger, der gør det muligt for den udenlandske myndighed at vurdere, om oplysningerne er rigtige, fuldstændige, ajourførte og pålidelige.

Hvis det konstateres, at der er videregivet urigtige personoplysninger, eller at oplysningerne er videregivet ulovligt, meddeles dette straks den udenlandske myndighed. Oplysningerne skal berigtiges, slettes eller blokeres omgående, jf. bekendtgørelsens § 9, stk. 2.

Det foreslås i *§ 4, stk. 5,* at den dataansvarlige skal træffe alle rimelige foranstaltninger til at sikre, at personoplysninger ikke videregives eller stilles til rådighed, hvis de er urigtige, ufuldstændige eller ikke ajourførte. I dette øjemed verificerer den dataansvarlige så vidt muligt kvaliteten af personoplysningerne, før de videregives eller stilles til rådighed. I forbindelse med videregivelse af oplysninger skal der så vidt muligt tilføjes nødvendige oplysninger, der gør det muligt for den modtagende kompetente myndighed at vurdere, i hvor høj grad personoplysningerne er rigtige,

fuldstændige og pålidelige, og i hvilket omfang de er ajourførte. Hvis det konstateres, at der er videregivet urigtige personoplysninger, eller at personoplysninger er videregivet ulovligt, skal dette straks meddeles modtageren. Oplysningerne skal i givet fald berigtiges, slettes eller behandlingen skal begrænses.

Den foreslåede bestemmelse udgør i nogen grad en præcisering af princippet i den foreslåede § 4, stk. 4, hvorefter det generelt skal sikres, at de oplysninger, som behandles, er korrekte.

Med den foreslåede bestemmelse præciseres det således, at den dataansvarlige navnlig i forbindelse med, at personoplysninger videregives og stilles til rådighed, skal sikres sig, at oplysningerne er korrekte, fuldstændige og ajourførte. Oplysninger, som kan gøre det muligt for den modtagende myndighed at vurdere, om oplysningerne er rigtige, fuldstændige og ajourførte, kan efter omstændigheder bestå i oplysninger om kilden til oplysningerne og om, hvornår de er indsamlet.

De kompetente myndigheder er allerede efter gældende ret underlagt en sådan forpligtelse i forhold til den grænseoverskridende udveksling af personoplysninger, men med den foreslåede bestemmelse udvides – den eksplicitte – forpligtelsen til rent nationale forhold.

Kravet vil dog fortsat navnlig være relevant i forbindelse med, at de danske kompetente myndigheder videregiver oplysninger til de kompetente myndigheder i andre medlemsstater, idet kravet om, at der skal ske berigtigelse, sletning eller begrænsning dog retter sig til danske kompetente myndigheder, som har modtaget oplysninger fra kompetente myndigheder i andre medlemsstater.

Bestemmelsens angivelse af, at den dataansvarlige skal tage visse skridt *så vidt muligt*, indebærer alene en overordnet pligt for den dataansvarlige til at have for øje, om de konkrete skridt – f.eks. at verificere personoplysninger inden en videregivelse – bør gennemføres under iagttagelse af de særlige forholdsregler, som bestemmelsen angiver. I den forbindelse vil den dataansvarlige efter omstændighederne kunne tage hensyn til bl.a. den konkrete videregivelse, modtageren af oplysningerne, til hvilke formål oplysningerne skal anvendes, om der er tale om en behandling, der er forudsat i lovgivningen, og om behandlingen i tidligere tilfælde har medført risici for de registrerede mv.

Der henvises i øvrigt til pkt. 2.3.3.4 i lovforslagets almindelige bemærkninger.

Til stk. 6

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

Det foreslås i *§ 4, stk. 6*, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Der er således tale om en videreførelse af gældende ret.

Der henvises i øvrigt til pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 7

Det fremgår af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Det foreslås i *§ 4, stk. 7*, at indsamlede oplysninger skal behandles på en måde, der sikrer en 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, jf. de foreslåede regler om behandlingssikkerhed i § 27.

Med den foreslåede bestemmelse præciseres det således allerede i forbindelse med de generelle behandlingsprincipper, at den dataansvarlige skal sikre, at behandlingen sker under anvendelse af passende fornødne tekniske og organisatoriske foranstaltninger.

Der henvises i øvrigt til pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 8

Persondataloven indeholder ikke en eksplicit og overordnet bestemmelse om den dataansvarliges ansvar. I stedet følger den dataansvarliges ansvar implicit af, at den dataansvarlige har retten til at disponere og bestemme over de pågældende personoplysninger og derfor også er ansvarlig for overholdelse af databeskyttelsesretten ved behandling af personoplysninger.

Det foreslås i *§ 4, stk. 8,* at den dataansvarlige er ansvarlig for og skal kunne påvise, at behandlingsprincipperne i den foreslåede § 4, stk. 1-7 overholdes.

Bestemmelsen indeholder det databeskyttelsesretlige princip om *ansvarlighed*. Dette princip indebærer, at den dataansvarlige i passende omfang skal kunne påvise, at de behandlinger af personoplysninger, der finder sted, er i overensstemmelse med stk. 1-7. Kravet om at påvise overholdelse må navnlig antages at indebære en mere generel pligt til over for tilsynsmyndigheden, på foranledning, at kunne godtgøre, at de relevante krav efterleves. Dette vil i praksis – som det i dag er tilfældet under persondataloven – kunne ske ved at stille den dataansvarliges sikkerhedspolitik og andre relevante interne regelsæt til rådighed. Kravet vil f.eks. også kunne imødekommes ved, at den dataansvarlige i relevant omfang godtgør, at der er taget skridt til at sikre en passende uddannelse og oplysning af medarbejderne om indholdet af de relevante krav, som loven og de relevante interne politikker indeholder.

Bestemmelsen indebærer på den anden side ikke krav om en meget udførlig og findelt dokumentation af enhver behandlingsaktivitet, som den dataansvarlige gennemfører. Der lægges i den forbindelse vægt på, at de kompetente myndigheder behandler en meget betydelig mængde personoplysninger på baggrund af et udførligt lovgrundlag og generelt – for politi og anklagemyndighedens vedkommende – er underlagt en særlig legalitetskontrol for så vidt angår de behandlinger, der finder sted som led i efterforskningen mv. af strafbare forhold, og som dermed tilrettelægges med henblik på at kunne tåle en nærmere retslig prøvelse. Det vil således under alle omstændigheder ikke bibringe væsentlig merværdi, såfremt f.eks. poli-

tiet var forpligtet til meget udførligt at beskrive, hvorfor konkrete personoplysninger behandles til brug for en given type straffesag mv.

Der henvises i øvrigt til pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger.

Til § 5

Til stk. 1

Det fremgår af persondatalovens § 5, stk. 2, 1. pkt., at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål.

Bestemmelsen er udtryk for det såkaldte finalité-princip, som indebærer, at indsamlingen af oplysninger skal ske med et bestemt formål for øje, og at der er visse grænser for, hvordan oplysningerne efterfølgende kan anvendes. Angivelsen af, at senere behandling blot ikke må være uforenelig med det oprindelige formål, indebærer dog, at der er en ret lempelig adgang for navnlig offentlige myndigheder til at behandle, herunder videregive, oplysninger til nye formål.

Det foreslås i *§ 5, stk. 1*, at senere behandling af oplysninger til et andet af de formål, der er nævnt i § 1, stk. 1, end det, hvortil de oprindeligt var indsamlet, kan foretages af den samme eller en anden af de kompetente myndigheder, når behandlingen sker på baggrund af lov og er nødvendig og forholdsmæssig i forhold til dette efterfølgende formål.

Den foreslåede bestemmelse giver således en relativt vid adgang for de kompetente myndigheder til at behandle, herunder videregive, oplysninger til nye formål inden for lovens anvendelsesområde.

Det er f.eks. relevant i forhold til den videregivelse af personoplysninger, som finder sted i forbindelse med en straffesags forløb. Politiet kan således indsamle oplysninger om en mistænkts telefonnummer i forbindelsen med efterforskningen af et strafbart forhold. Hvis der indledes en straffesag, vil oplysningen om den (nu) tiltaltes telefonnummer blive videregivet til domstolene til brug for forkyndelse af anklageskrift og indkaldelse til hovedforhandling. Hvis den pågældende findes skyldig og idømmes en fængselsstraf, vil oplysningerne om den (nu) dømtes telefonnummer blive videregivet til kriminalforsorgen til brug for indkaldelse til afsoning.

Såfremt det efterfølgende formål falder uden for lovens anvendelsesområde, vil behandlingen, herunder den kompetente myndigheds videregivelse, skulle ske på baggrund af persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen.

Der henvises i øvrigt til pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 2

Det fremgår af persondatalovens § 5, stk. 2, 2. pkt., at senere behandling af oplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, ikke anses for uforenelig med de formål, hvortil oplysningerne er indsamlede.

Det fremgår videre af persondatalovens § 14, at oplysninger, der er omfattet af persondataloven, kan overføres til arkiv efter reglerne i arkivlovgivningen.

Det foreslås i *§ 5, stk. 2*, at der i medfør af stk. 1 kan foretages behandling af oplysninger, der alene sker til arkivformål i samfundets interesse eller i historisk, statistisk eller videnskabeligt øjemed.

Med den foreslåede bestemmelse gøres det klart, at en behandling, der alene sker til arkivformål i samfundets interesse eller i historisk, statistisk eller videnskabeligt øjemed, opfylder betingelsen i den foreslåede § 5, stk. 1, om, at en efterfølgende behandling skal være nødvendig og forholdsmæssig.

Bestemmelsen omfatter alene behandling, der er omfattet af lovens anvendelsesområde. I det omfang, at der er tale om behandling med henblik på arkivformål i samfundets interesse eller i historisk, statistisk eller videnskabeligt øjemed, som falder uden for lovens anvendelsesområde, vil behandlingen, herunder videregivelsen, i stedet skulle ske efter de ovennævnte regler i persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen.

Til stk. 3

Persondataloven indeholder ikke et en eksplicit og overordnet bestemmelse om den dataansvarliges ansvar. I stedet følger den dataansvarliges ansvar implicit af, at den dataansvarlige har retten til at disponere og bestemme over de pågældende personoplysninger og derfor også er ansvarlig for overholdelse af databeskyttelsesretten ved behandling af personoplysninger.

Det foreslås i *§ 5, stk. 3,* at den dataansvarlige er ansvarlig for og skal kunne påvise, at en efterfølgende behandling er i overensstemmelse med den foreslåede § 5, stk. 1 og 2, jf. herved også den foreslåede § 4, stk. 8. og bemærkningerne hertil.

Der henvises i øvrigt til pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger.

Til § 6

Det fremgår af rammeafgørelsesbekendtgørelsens § 3, stk. 3, at behandling ikke må ske i strid med specifikke begrænsninger for behandling af videregivne oplysninger fastsat i lovgivningen gældende for den videregivende udenlandske myndighed, når den videregivende myndighed gør opmærksom på begrænsningerne.

Det foreslås i *stk. 1,* at når der foretages videregivelse, fastsætter og underretter den videregivende kompetente myndighed om eventuelle særlige vilkår for behandling af oplysninger. Der kan ikke fastsættes særlige vilkår alene som følge af, at der er tale om en videregivelse til en modtager i en anden medlemsstat.

Den foreslåede bestemmelse vedrører både videregivelse mellem de kompetente danske myndigheder og videregivelse fra en dansk kompetent myndighed til en kompetent myndighed i anden medlemsstat.

Bestemmelsen giver mulighed for, at de kompetente myndigheder i Danmark kan opstille de samme vilkår for, hvordan henholdsvis en anden dansk kompetent myndighed og en kompetent myndighed i en anden medlemsstat kan behandle, herunder navnlig videregive, personoplysninger. Der kan f.eks. være tale om et forbud mod at videregive personoplysninger til andre, eller at anvende oplysningerne til andre formål end dem, på baggrund af hvilke de blev videregivet til modtageren.

Det foreslås videre i *stk. 2*, at behandling af oplysninger, der er modtaget fra en kompetent myndighed, ikke må ske i strid med særlige vilkår, som er fastsat af den videregivende kompetente myndighed.

Med den foreslåede bestemmelse sikres det, at de kompetente myndigheder er forpligtet til at overholde eventuelle særlige vilkår, som er fastsat af den videregivende myndighed. Det er en forudsætning, at den videregivende myndighed har gjort opmærksom på det særlige vilkår, eller det på anden måde står klart for den modtagende myndighed, at der gælder særlige vilkår for behandlingen af de modtagne personoplysninger.

Til § 7

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

Det fremgår af rammeafgørelsesbekendtgørelsens § 8, at den dataansvarlige skal tilrettelægge behandlingen af personoplysninger således, at der fastsættes passende frister for sletningen af personoplysninger eller regelmæssig undersøgelse af behovet for lagringen af oplysningerne. Det sikres endvidere ved proceduremæssige foranstaltninger, at tidsfristerne overholdes.

Det foreslås i *§ 7*, at den dataansvarlige skal tilrettelægge behandlingen af personoplysninger således, at der fastsættes passende frister for sletningen af personoplysninger eller regelmæssig undersøgelse af behovet for lagringen af oplysningerne. Det sikres endvidere ved proceduremæssige foranstaltninger, at tidsfristerne overholdes.

De kompetente myndigheder er allerede efter gældende ret underlagt en sådan forpligtelse i forhold til den grænseoverskridende udveksling af personoplysninger, men med den foreslåede bestemmelse udvides – den eksplicitte – forpligtelsen til rent nationale forhold.

Kravet vil kunne opfyldes ved, at den dataansvarlige myndighed fastsætter generelle frister for, hvornår de personoplysninger, som myndigheden behandler, skal slettes.

Der er således ikke krav om, at den dataansvarlige løbende skal gennemgå samtlige sine sager, dokumenter mv. med henblik på at sikre, at der ikke opbevares konkrete personoplysninger i strid med bestemmelsen, så længe myndigheden har procedurer, som sikrer, at der sker sletning i overensstemmelse med de fastsatte frister.

Der henvises i øvrigt til pkt. 2.3.3.2 i lovforslagets almindelige bemærkninger.

Til § 8

Gældende ret indeholder ikke en eksplicit forpligtelse for den dataansvarlige til at sondre mellem forskellige kategorier af registrerede.

Det foreslås i *§ 8*, at den dataansvarlige, når det er relevant, så vidt muligt skal sondre mellem personoplysninger om forskellige kategorier af registrerede, herunder personer, om hvem der er væsentlig grund til at tro, at de har begået eller vil begå en strafbar handling, personer, der er dømt for en strafbar handling, ofre for en strafbar handling eller personer, om hvem visse faktiske omstændigheder giver anledning til at tro, at de kunne blive ofre for en strafbar handling, og andre parter i forbindelse med en strafbar handling, såsom personer, der kan blive indkaldt som vidner i efterforskninger i forbindelse med strafbare handlinger eller i efterfølgende straffesager, personer, der kan tilvejebringe oplysninger om strafbare handlinger, eller kontakt- eller ledsagepersoner for personer, om hvem der er væsentlig grund til at tro, at de har begået eller vil begå en strafbar handling, eller personer, der er dømt for en strafbar handling,

Kravet vil efter omstændighederne fortsat kunne opfyldes på forskellige måder. Der vil således kunne ske en opfyldelse af kravet ved at anvende forskellige databehandlingssystemer eller forskellige generelle regler for forskellige kategorier af registrerede. Det vil endvidere kunne opfyldes gennem konkrete angivelser af, hvilken kategori af en registreret som en given oplysning vedrører, hvilket muliggør, at der vil kunne foretages en konkret afvejning, inden der iværksættes behandling. Angivelsen af, at der *så vidt muligt* skal sondres, indebærer dog, at der f.eks. i de fleste sammenhænge ikke skal ske en forskellig behandling af oplysninger om forskellige kategorier af registrerede i den samme politirapport.

Angivelsen af, at der skal sondres, når det er relevant, indebærer, at der kan være situationer, hvor der ikke skal sondres mellem forskellige kate-

gorier af registrerede. Der kan f.eks. være tale om en behandling af personoplysninger, som varetager et så tungtvejende hensyn, f.eks. efterforskning af alvorlig kriminalitet, at der ikke er krav om at foretage en sondring mellem de forskellige kategorier af registrerede, som oplysningerne vedrører.

Der henvises i øvrigt til pkt. 2.3.3.3 i lovforslagets almindelige bemærkninger.

Til § 9

Det fremgår af persondatalovens § 6, at behandling af personoplysninger kan ske, når den registrerede har meddelt samtykke hertil (stk. 1, nr. 1), når behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige (stk. 1, nr. 3), når behandlingen er nødvendig for at beskytte den registreredes vitale interesser (stk. 1, nr. 4), når behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige er pålagt (stk. 1, nr. 6), og/eller når behandling er nødvendig af hensyn til en berettiget interesse og hensynet til den registrerede ikke overstiger denne interesse (stk. 1, nr. 7).

Det foreslås i *§ 9*, at behandling af oplysninger må kun finde sted, når behandlingen er nødvendig for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

Den foreslåede bestemmelse erstatter således de behandlingsgrundlag efter persondataloven, som de kompetente myndigheder i dag anvender til behandling af personoplysninger, herunder personnumre.

Der henvises i øvrigt til pkt. 2.3.3.5 i lovforslagets almindelige bemærkninger.

Til § 10

Det fremgår af persondatalovens § 7 stk. 1, at der som hovedregel ikke må behandles oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

Det fremgår videre af bestemmelsens stk. 6, at behandling af de følsomme oplysninger, der er nævnt i stk. 1, kan ske, hvis behandlingen er nødvendig af hensyn til en offentlig myndigheds varetagelse af sine opgaver på det strafferetlige område.

Persondatalovens § 7, stk. 6, suppleres for så vidt angår grænseoverskridende udveksling af oplysninger af rammeafgørelsesbekendtgørelsens § 2, stk. 2. Det fremgår heraf, at behandling af oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold efter persondatalovens § 7, stk. 6, ikke må ske, medmindre behandlingen er strengt nødvendig.

Det foreslås i *§ 10, stk. 1*, at der ikke må behandles 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.

Det foreslås videre i *§ 10, stk. 2*, at der dog under overholdelse af betingelserne i lovforslaget kan foretages behandling af oplysninger omfattet af stk. 1, når det er strengt nødvendigt og sker af hensyn til de formål, der er nævnt i § 1, stk. 1, herunder for at beskytte den registreredes eller en anden fysisk persons vitale interesser, eller hvis behandlingen vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede.

I forhold til behandlingen af almindelige personoplysninger, er der således efter den foreslåede bestemmelse tale om et skærpet krav til nødvendigheden, idet behandlingen for så vidt angår disse særlige kategorier af oplysninger skal være strengt nødvendig. Kravet er desuden skærpet i forhold til den gældende bestemmelse i persondatalovens § 7, stk. 6, men er en videreførelse af kravet i rammeafgørelsesbekendtgørelsens § 2, stk. 2.

I praksis vil det dog formentlig ikke vil være muligt at angive nogen væsentlig forskel på kriterierne ”nødvendigt” og ”strengt nødvendigt”. Det gælder således bl.a. i relation til politiets mv. adgang til at behandle de nævnte typer af følsomme personoplysninger med henblik på kriminalitetsbekæmpelse, f.eks. behandling af oplysninger om politisk overbevisning i forbindelse med opklaring af et politisk motiveret mord, eller be-

handling af oplysninger om race med henblik på at identificere en gerningsmand.

Henvisningen til, at der kan ske behandling for at beskytte den registreredes eller en anden fysisk persons vitale interesser, eller hvis der er tale om oplysninger, som tydeligvis er offentliggjort af den registrerede er medtaget for at sikre, at der ikke kan opstå tvivl om, hvorvidt der er sket en korrekt implementering af retshåndhævelsesdirektivets artikel 10.

Der henvises i øvrigt til pkt. 2.3.3.6 i lovforslagets almindelige bemærkninger.

Til § 11

Det fremgår af persondatalovens § 39, at hvis en registreret person fremsætter indsigelse herimod, kan den dataansvarlige ikke foranstalte, at den registrerede undergives afgørelser, der har retsvirkninger for eller i øvrigt berører den pågældende i væsentlig grad, og som alene er truffet på grundlag af elektronisk databehandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold.

Efter bestemmelsens stk. 3 har den registrerede ret til hos den dataansvarlige snarest muligt og uden ugrundet ophold at få at vide, hvilke beslutningsregler der ligger bag en afgørelse som nævnt i stk. 1. Persondatalovens § 30 om undtagelser fra oplysningspligten finder tilsvarende anvendelse.

Persondatalovens § 30 finder ikke anvendelse for politiets, anklagemyndighedens og domstolenes behandling af personoplysninger inden for det strafferetlige område.

Det foreslås i *§ 11, stk. 1,* at der kan træffes afgørelser, der har negativ retsvirkning for den registrerede eller betydeligt påvirker den pågældende, alene på grundlag af automatisk behandling, herunder profilering.

Det er en betingelse, at der findes passende foranstaltninger til at sikre den registreredes berettigede interesser, herunder i det mindste en ret for den registrerede til at kræve menneskelig indgriben fra den dataansvarliges side, jf. den foreslåede *§ 11, stk. 2*.

Det foreslås endvidere i *§ 11, stk. 3*, at justitsministeren bemyndiges til at fastsætte nærmere regler om foranstaltninger omfattet af stk. 2.

Der træffes ikke aktuelt sådanne afgørelser af de kompetente myndigheder, men hvis det i fremtiden måtte blive relevant, navnlig som følge af den teknologiske udvikling, etableres der med den foreslåede bestemmelse en mulighed herfor.

De afgørelser, som i givet fald vil være omfattet af bestemmelsen, vil være myndighedsafgørelser i forvaltningslovens forstand, dvs. udtalelser, der går ud på at fastsætte, hvad der er eller skal være ret i et foreliggende tilfælde, idet automatiske afgørelser ikke er relevante i forhold til afgørelser truffet af domstolene.

De foranstaltninger, som justitsministeren vil kunne fastsætte nærmere regler om, kan udover adgangen til at kræve menneskelig indgriben f.eks. være regler om, at der stikprøvevis skal foretages en menneskelig kontrol af de automatiske afgørelser.

Der henvises i øvrigt til pkt. 2.3.3.7 i lovforslagets almindelige bemærkninger.

Til § 12

Gældende ret indeholder ikke en forpligtelse for den dataansvarlige til at indføre mekanismer, som kan tilskynde til indberetning af overtrædelse af reglerne om beskyttelse af personoplysninger.

Det foreslås i *§ 12*, at de kompetente myndigheder skal indføre effektive mekanismer, som tilskynder til fortrolig indberetning til tilsynsmyndighederne af overtrædelser af den foreslåede lov.

Der kræves ikke etablering af egentlige whistle-blower-ordninger for at opfylde kravet. En mekanisme kan således f.eks. bestå i, at det sikres, at ansatte – eventuelt via databeskyttelsesrådgiveren – kan indberette en overtrædelse af loven – eller en formodning herom – til tilsynsmyndigheden, såfremt der er truffet foranstaltninger, der sikrer, at dette ikke vil føre til disciplinære reaktioner over for de pågældende.

Til § 13

Det fremgår af persondatalovens § 28, stk. 1, at den dataansvarlige eller dennes repræsentant ved indsamling af oplysninger hos den registrerede skal give den registrerede meddelelse om den dataansvarliges og dennes repræsentants identitet, formålene med den behandling, hvortil oplysningerne er bestemt, og alle yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser, som f.eks. kategorierne af modtagere, om det er obligatorisk eller frivilligt at besvare stillede spørgsmål samt mulige følger af ikke at svare, og om reglerne om indsigt i og om berigtigelse af de oplysninger, der vedrører den registrerede. Bestemmelsen i stk. 1 gælder ikke, hvis den registrerede allerede er bekendt med disse oplysninger, jf. stk. 2.

Det fremgår videre af persondatalovens § 29, stk. 1, at hvor oplysninger ikke er indsamlet hos den registrerede, påhviler det den dataansvarlige eller dennes repræsentant ved registreringen, eller hvor de indsamlede oplysninger er bestemt til videregivelse til tredjemand, senest når videregivelsen af oplysningerne finder sted, at give den registrerede meddelelse om den dataansvarliges og dennes repræsentants identitet, formålene med den behandling, hvortil oplysningerne er bestemt, og alle yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser, som f.eks. hvilken type oplysninger det drejer sig om, kategorierne af modtagere og om reglerne om indsigt i og om berigtigelse af de oplysninger, der vedrører den registrerede. Bestemmelsen i stk. 1 gælder ikke, hvis den registrerede allerede er bekendt med disse oplysninger, hvis registreringen eller videregivelsen udtrykkeligt er fastsat ved lov eller bestemmelser fastsat i henhold til lov, eller hvis underretning af den registrerede viser sig umulig eller er uforholdsmæssigt vanskelig, jf. stk. 2 og 3.

Det foreslås i *§ 13, stk. 1,* at den dataansvarlige skal stille følgende oplysninger til rådighed for den registrerede:

1) Identitet på og kontaktoplysninger for den dataansvarlige.
2) Kontaktoplysninger for databeskyttelsesrådgiveren og oplysninger om dennes funktion i forhold til de registrerede.
3) Formålene med den behandling, som personoplysningerne skal bruges til.
4) Retten til at indgive en klage til en tilsynsmyndighed og kontaktoplysningerne for tilsynsmyndigheden.
5) Den registreredes rettigheder efter kapitel 5 og 6.

6) Retten til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder i forhold til de kompetente myndigheders afgørelser om undladelse, udsættelse, begrænsning eller nægtelse efter kapitel 4-6, jf. § 40, stk. 1, nr. 9.

Den dataansvarliges forpligtelse til at stille oplysninger til rådighed kan f.eks. opfyldes ved at gøre oplysningerne tilgængelige på den kompetente myndigheds hjemmeside eller gennem trykt materiale, som er tilgængeligt for de registrerede.

Navnlig for så vidt angår kravet i bestemmelsens *nr. 3*, hvorefter den dataansvarlige skal angive formålene med den behandling, som personoplysningerne skal bruges til, vil en mere generel angivelse af de opgaver som myndigheden varetager anses for at være tilstrækkelig. Det vil således f.eks. i forhold til en dataansvarlig politimyndighed være tilstrækkeligt, hvis det fremgår af de oplysninger, der stilles til rådighed, at oplysninger behandles med henblik på at løse de opgaver, der fremgår af politilovens § 2, kombineret med en nærmere angivelse af hvilke opgaver, der fremgå af politilovens § 2.

Bestemmelsen i *stk. 2* indebærer en pligt for den dataansvarlige til at meddele en række oplysninger til den registrerede i konkrete sager.

Det foreslås således i *§ 13, stk. 2*, at når det er nødvendigt for, at den registrerede kan varetage sine interesser, skal den dataansvarlige som minimum give den registrerede meddelelse om følgende:

1) Retsgrundlaget for behandlingen.
2) Det tidsrum, hvor personoplysningerne vil blive opbevaret, eller, hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum.
3) Kategorierne af eventuelle modtagere af personoplysningerne, herunder i tredjelande eller internationale organisationer.
4) Hvis det er nødvendigt, yderligere oplysninger, navnlig hvis personoplysningerne indsamles uden den registreredes vidende.

Efter den foreslåede bestemmelse stilles der – i modsætning til efter den foreslåede § 13, stk. 1 – krav om, at den dataansvarlige myndighed konkret underretter den registrerede. Bestemmelsen vil finde anvendelse i de tilfælde, hvor en dataansvarlig behandler en konkret straffesag mv.

Underretning skal ske, når det er nødvendigt under hensyntagen til de specifikke omstændigheder, hvorunder oplysningerne behandles, med henblik på at sikre den registrerede en rimelig behandling af oplysningerne. Der vil imidlertid skulle tages behørigt hensyn til f.eks. de særlige fortrolighedshensyn, som politiet og anklagemyndighedens behandling af personoplysninger om mistænkte mv. er underlagt i forbindelse med en straffesags efterforskning og forberedelse, jf. også bemærkningerne til lovens § 14.

Det vil ikke være nødvendigt at foretage underretning af den registrerede, hvis der er tale om en sammenhæng, hvor behandlingen af oplysningerne ikke kan føre til negative retsvirkninger for den registrerede, eller hvis det ud fra sammenhængen, hvori oplysningerne er indsamlet, må stå klart for den registrerede, hvad oplysningerne skal anvendes til, f.eks. et vidne, der til brug for en konkret efterforskning afgiver forklaring til politiet. Tilsvarende vil gælde behandling af oplysninger vedrørende personer, som utilsigtet eller tilfældigt kommer i berøring med en konkret straffesag, f.eks. i forbindelse med overvågning, aflytning og lignende af en person, som er mistænkt for et strafbart forhold.

Underretningen skal ske ved indsamlingen eller i umiddelbar forlængelse heraf. Der skal ske underretning, uanset om oplysningerne indsamles med eller uden den pågældendes vidende.

Der er ingen formkrav til underretningen, men hensynet til at sikre, at der ikke kan opstå tvivl om, hvorvidt der er foretaget korrekt underretning, fører til, at underretningen som udgangspunkt bør ske skriftligt.

Kravet i *nr. 1* om, at retsgrundlaget for behandlingen skal meddeles til den registrerede, kan opfyldes gennem en angivelse af den lovbestemmelse, der danner grundlag for den relevante behandling af personoplysninger. Alt efter de konkrete omstændigheder kan retsgrundlaget være en generel lovhjemlet opgave, som f.eks. de opgaver, der fremgår af politilovens § 2, eller være knyttet til mere konkrete opgaver, sagstyper mv., som den dataansvarlige varetager. Det afgørende for, om kravet kan anses for opfyldt, vil være, om den registrerede tilvejebringes en mulighed for at gøre sig bekendt med det retlige grundlag for behandlingen af personoplysninger.

Underretningen skal ikke indeholde oplysninger om, hvilke konkrete oplysninger der behandles om den pågældende. Ønsker den registrerede oplysninger herom, skal det ske i medfør af den foreslåede § 15 om den registreredes indsigtsret.

Hvis der er tale om en løbende indsamling af oplysninger, er det tilstrækkeligt, hvis underretningen gives én gang, eller at en tidligere meddelt underretning suppleres.

For så vidt angår kravet om, at der skal gives yderligere oplysninger, når det er nødvendigt, jf. *nr. 4*, kan der f.eks. være tale om oplysninger om, at den registrerede vil blive underlagt en automatisk afgørelse efter den foreslåede § 11.

Der henvises i øvrigt til pkt. 2.4.3.1 i lovforslagets almindelige bemærkninger.

Til § 14

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

Undtagelse fra bestemmelserne i § 28, stk. 1, og § 29, stk. 1, 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 statens sikkerhed (nr. 1), forsvaret (nr. 2), den offentlige sikkerhed (nr. 3), forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv (nr. 4), væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender (nr. 5), og kontrol-, tilsyns- eller reguleringsopgaver, herunder opgaver af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i nr. 3-5 nævnte områder (nr. 6).

Det foreslås i *§ 14, stk. 1*, at meddelelse efter den foreslåede § 13, stk. 2, kan udsættes, begrænses eller undlades, hvis det følger af lov, eller hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for at

1) undgå, at der lægges hindringer i vejen for officielle eller retlige undersøgelser, efterforskninger eller procedurer,
2) undgå at skade forebyggelsen, afsløringen, efterforskningen eller retsforfølgningen af strafbare handlinger eller fuldbyrdelsen af strafferetlige sanktioner,

3) beskytte den offentlige sikkerhed,
4) beskytte statens sikkerhed, eller
5) beskytte den registreredes eller andres rettigheder.

Med den foreslåede bestemmelse gives der mulighed for at udsætte, begrænse eller undlade en underretning af den registrerede.

Som følge af det foreslåede anvendelsesområde for loven, vil navnlig hensynet til at undgå, at der lægges hindringer i vejen for officielle eller retlige undersøgelser, efterforskninger eller procedurer, jf. *nr. 1*, og hensynet til at undgå at skade forebyggelsen, afsløringen, efterforskningen eller retsforfølgningen af strafbare handlinger eller fuldbyrdelsen af strafferetlige sanktioner, jf. *nr. 2*, ofte føre til, at der ikke skal gives underretning til den registrerede i medfør af den foreslåede § 13, stk. 2. Der kan f.eks. være tale om situationer, hvor en meddelelse til den registrerede om, at politiet i forbindelse med en efterforskning behandler oplysninger om den pågældende, f.eks. i form af en aflytning, vil indebære, at formålet med efterforskningen forspildes.

Begrænsninger i underretningspligten, som følger af eksisterende lovgivning, herunder retsplejelovens regler, vil kunne opretholdes, såfremt begrænsningen sker af hensyn til en af de grunde, som fremgår af den foreslåede § 14, stk. 2, jf. herved også den foreslåede § 2 og bemærkningerne hertil.

Det foreslås videre i *§ 14, stk. 2*, at justitsministeren bemyndiges til at fastsætte nærmere regler om, hvilke kategorier af behandling der er omfattet af stk. 1, samt om, at meddelelse efter § 13, stk. 2, kan udsættes til et passende tidspunkt, for så vidt hensynene i stk. 1 må antages at medføre, at meddelelser i almindelighed må underkastes en sådan udsættelse.

Adgangen for justitsministeren til at fastsætte nærmere regler om, at meddelelse efter § 13, stk. 2, kan udsættes til et passende tidspunkt, vil navnlig kunne anvendes til at fastsætte regler om, at meddelelse bør finde sted samtidig med de øvrige processuelle skridt, som straffesager er underlagt. I praksis vil de hensyn, som fremgår af den foreslåede § 14, stk. 1, føre til, at oplysningspligten efter § 13, stk. 1, ikke kan iagttages tidligere end det tidspunkt, hvor der eksempelvis rejses sigtelse, og hvor der således gives meddelelse til den pågældende i overensstemmelse med retsplejelovens regler herom. Efter bestemmelsen vil justitsministeren således kunne regulere nærmere, hvornår lignende tilfælde må antages at foreligge inden for

lovens anvendelsesområde, samt hvordan meddelelse i sådanne tilfælde skal gennemføres mv.

Den registreredes ret til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder i forhold til udsættelse, begrænsning eller nægtelse finder fortsat anvendelse, uanset at en udsættelse af tidspunktet for meddelelse efter § 13, stk. 2, følger af en sådan generelt fastsat regel.

Der henvises i øvrigt til pkt. 2.4.3.1 i lovforslagets almindelige bemærkninger.

Til § 15

Det fremgår af persondatalovens § 31, at når en person fremsætter begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om, hvilke oplysninger der behandles, behandlingens formål, kategorierne af modtagere af oplysningerne og tilgængelig information om, hvorfra disse oplysninger stammer.

Den dataansvarlige skal snarest besvare begæringer som nævnt i stk. 1. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om, hvornår afgørelsen kan forventes at foreligge, jf. stk. 2.

Det foreslås i *§ 15, stk. 1*, at hvis en registreret fremsætter begæring herom, skal den dataansvarlige bekræfte over for den pågældende, om der behandles oplysninger om vedkommende.

Behandles der oplysninger om den pågældende, skal der efter den foreslåede *§ 15, stk. 2*, gives adgang til oplysningerne samt en meddelelse med følgende oplysninger:

1) Formålene med og retsgrundlaget for behandlingen.
2) De berørte kategorier af personoplysninger.
3) De modtagere eller kategorier af modtagere, som personoplysningerne er videregivet til, navnlig modtagere i tredjelande eller internationale organisationer.
4) Om muligt, det påtænkte tidsrum, hvor personoplysningerne vil blive opbevaret, eller, hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum.

5) Retten til at anmode den dataansvarlige om berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede.
6) Retten til at indgive en klage til tilsynsmyndigheden og kontaktoplysningerne for tilsynsmyndigheden.
7) Hvilke personoplysninger, der er omfattet af behandlingen, og enhver tilgængelig oplysning om, hvorfra de stammer.

De oplysninger, der efter bestemmelsen skal meddeles til den registrerede, er de oplysninger, der behandles på tidspunktet for begæringen og indtil begæringen ekspederes. Den registrerede har ikke krav på at få oplyst, hvilke oplysninger der tidligere har været undergivet behandling.

Formålet med behandlingen, jf. *nr. 1*, kan angives generelt, f.eks. "til brug for efterforskning af strafbare forhold".

Hvis der hersker rimelig tvivl om identiteten af den fysiske person, der fremsætter en indsigtsanmodning, skal den dataansvarlige i overensstemmelse med de almindelige forvaltningsretlige principper anmode om de yderligere oplysninger, der er nødvendige for at bekræfte den pågældendes identitet.

Til § 16

Persondatalovens § 32 indeholder en række undtagelser til indsigtsretten efter § 31. Det fremgår således af bestemmelsens stk. 1, at retten til indsigt ikke gælder, hvis betingelserne i § 30 er opfyldt, jf. ovenfor.

Det fremgår videre af bestemmelsens 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.

Bestemmelsen i § 31, stk. 1, finder heller ikke 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, jf. stk. 4.

Det fremgår desuden af bestemmelsens stk. 5, at for behandling af oplysninger på det strafferetlige område, der foretages for den offentlige forvaltning, kan justitsministeren fastsætte undtagelser fra retten til at få oplysninger efter § 31, stk. 1, for så vidt bestemmelsen i § 32, stk. 1, jf. herved § 30, må antages at medføre, at begæringer om ret til indsigt i almindelighed må afslås.

Justitsministeren har anvendt bemyndigelsesbestemmelsen i lovens § 32, stk. 5, til at udstede en række bekendtgørelser, herunder bekendtgørelse nr. 1776 af 16. december 2015 om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG), hvorefter indsigtsretten ikke finder anvendelse i forhold til oplysninger i ANPG-systemet, jf. bekendtgørelsens § 13.

Det foreslås i *§ 16, stk. 1*, at indsigt efter § 15 kan udsættes, begrænses eller nægtes, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for de hensyn til offentlige interesser, der er nævnt i § 14, stk. 1.

Med den foreslåede bestemmelse gives der mulighed for at udsætte, begrænse eller undlade at give den registrerede indsigt.

Som følge af det foreslåede anvendelsesområde for loven vil navnlig hensynet til at undgå, at der lægges hindringer i vejen for officielle eller retlige undersøgelser, efterforskninger eller procedurer, jf. *nr. 1*, og hensynet til at undgå at skade forebyggelsen, afsløringen, efterforskningen eller retsforfølgningen af strafbare handlinger eller fuldbyrdelsen af strafferetlige sanktioner, jf. *nr. 2*, ofte føre til, at der ikke skal meddeles indsigt til den registrerede i medfør af den foreslåede § 16. Der kan f.eks. være tale om situationer, hvor den omstændighed, at den registrerede bliver bekendt med, at politiet i forbindelse med en efterforskning behandler oplysninger om den pågældende, f.eks. i form af en aflytning, vil indebære, at formålet med efterforskningen forspildes.

Begrænsninger i indsigtsretten, som følger af eksisterende lovgivning, herunder retsplejelovens regler, vil kunne opretholdes, såfremt begrænsningen sker af hensyn til en af de grunde, som fremgår af den foreslåede § 16, jf. herved også den foreslåede § 2 og bemærkningerne hertil.

Det foreslås endvidere i *§ 16, stk. 2*, at en afgørelse om, at den registreredes indsigt udsættes, begrænses eller nægtes, skal meddeles den registrerede skriftligt og skal være ledsaget af en begrundelse og en klagevejledning

samt oplysninger om den registreredes ret til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder i forhold til udsættelse, begrænsning eller nægtelse, jf. den foreslåede § 40, stk. 1, nr. 9.

Bestemmelsen skal forstås i lyset af de almindelige regler i forvaltningslovens kapitler 6 og 7 om begrundelse og klagevejledning, idet det dog efter den foreslåede bestemmelse er obligatorisk for den dataansvarlige at give en skriftlig begrundelse, ligesom der er et særligt krav om at oplyse om muligheden for, at den registrerede kan udøve sin indsigtsret gennem tilsynsmyndigheden.

Det foreslås videre i *§ 16, stk. 3*, at af hensyn til de i stk. 1 nævnte formål kan den registrerede i stedet for meddelelse efter stk. 2 gives meddelelse om, at det ikke kan oplyses, om der behandles oplysninger om den pågældende. En sådan meddelelse skal indeholde en klagevejledning og oplysninger om den registreredes ret til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder, jf. § 40, stk. 1, nr. 9.

Den kompetente myndighed vil efter den foreslåede bestemmelse således kunne svare den registrerede, at det hverken kan af- eller bekræftes, at der behandles oplysninger om den pågældende. Den foreslåede bestemmelse indebærer derimod ikke, at den dataansvarlige kan undlade at give en klagevejledning samt oplyse om den registreredes mulighed for at udøve sin indsigtsret gennem tilsynsmyndigheden.

Det foreslås endeligt i *§ 16, stk. 4*, at justitsministeren bemyndiges til at fastsætte nærmere regler om, hvilke kategorier af behandling der er omfattet af stk. 1, samt om undtagelse fra retten til at få oplysninger efter § 15 for så vidt hensynene i stk. 1 må antages at medføre, at begæringer om indsigt i almindelighed må afslås.

Den registreredes ret til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder i forhold til udsættelse, begrænsning eller nægtelse, jf. § 16, stk. 2, finder fortsat anvendelse, uanset om et afslag på indsigt følger af en sådan generelt fastsat regel.

Der henvises i øvrigt til pkt. 2.4.3.2 i lovforslagets almindelige bemærkninger.

Til § 17

Til stk. 1

Det fremgår af persondatalovens § 37, at den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Bestemmelsen finder generelt ikke anvendelse for politiets, anklagemyndighedens og domstolenes behandling af personoplysninger inden for det strafferetlige område, jf. persondatalovens § 2, stk. 4, men bestemmelsen finder dog anvendelse i forbindelse med den grænseoverskridende udveksling af personoplysninger, jf. rammeafgørelsesbekendtgørelsens § 2, stk. 4.

Det foreslås i *§ 17, stk. 1*, at den dataansvarlige efter anmodning fra den registrerede uden unødig forsinkelse skal berigtige oplysninger, der viser sig urigtige. På tilsvarende måde skal der ske fuldstændiggørelse af ufuldstændige oplysninger, hvis dette kan ske uden at bringe formålet med behandlingen i fare. Den dataansvarlige skal meddele berigtigelse af urigtige personoplysninger til den kompetente myndighed, hvorfra de urigtige oplysninger stammer.

Med den foreslåede bestemmelse sker der således i vidt omfang en videreførelse af de gældende regler om berigtigelse, som dog fremover tillige vil finde anvendelse i rent nationale forhold.

Retten til berigtigelse giver ikke den registrerede mulighed for at korrigere indholdet af f.eks. et vidneudsagn, idet spørgsmålet om, hvorvidt de personoplysninger, som fremgår af et vidneudsagn, er korrekte, skal håndteres i forbindelse med en straffesags behandling ved domstolene, jf. også den foreslåede § 17, stk. 3, nr. 2.

Den foreslåede bestemmelse skal endvidere ses i sammenhæng med den foreslåede § 4, stk. 1, om, at der ved behandlingen skal tages hensyn til oplysningernes karakter, hvoraf det følger, at der skal sondres mellem personoplysninger, der bygger på faktiske omstændigheder, og personoplysninger, der bygger på personlige vurderinger.

Dette har betydning i forhold til vurderingen af oplysningernes rigtighed. Navnlig i retssager er udsagn, der indeholder personoplysninger, baseret på en subjektiv opfattelse af fysiske personer, og det er ikke altid muligt at kontrollere dem. Kravet om oplysningernes rigtighed bør derfor ikke ved-

røre et udsagns rigtighed, men blot det forhold, at der er fremsat et konkret udsagn.

Adgangen til fuldstændiggørelse kan ske ved, at den registrerede fremlægge en supplerende erklæring, som kan knyttes til de oplysninger, som den dataansvarlige myndighed har om den registrerede.

Hvis der hersker rimelig tvivl om identiteten af den fysiske person, der fremsætter en anmodning, skal den dataansvarlige i overensstemmelse med de almindelige forvaltningsretlige principper anmode om de yderligere oplysninger, der er nødvendige for at bekræfte den pågældendes identitet.

Der henvises i øvrigt til pkt. 2.4.3.3 i lovforslagets almindelige bemærkninger.

Til stk. 2

Det fremgår af persondatalovens § 37, at den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Bestemmelsen finder generelt ikke anvendelse for politiets, anklagemyndighedens og domstolenes behandling af personoplysninger inden for det strafferetlige område, jf. persondatalovens § 2, stk. 4, men bestemmelsen finder dog anvendelse i forbindelse med den grænseoverskridende udveksling af personoplysninger, jf. rammeafgørelsesbekendtgørelsens § 2, stk. 4.

Det foreslås i *§ 17, stk. 2,* at den dataansvarlige efter anmodning fra den registrerede uden unødig forsinkelse skal slette oplysninger, der er behandlet i strid med behandlingsreglerne i kapitel 3, eller hvis det er påkrævet for at overholde en retlig forpligtelse, som den dataansvarlige er underlagt.

Med den foreslåede bestemmelse sker der således i vidt omfang en videreførelse af de gældende regler om berigtigelse, som dog fremover for så vidt angår politiet, anklagemyndigheden og domstolene tillige vil finde anvendelse i rent nationale forhold.

Der henvises i øvrigt til pkt. 2.4.3.3 i lovforslagets almindelige bemærkninger.

Til stk. 3

Det fremgår af persondatalovens § 37, at den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Bestemmelsen finder generelt ikke anvendelse for politiets, anklagemyndighedens og domstolenes behandling af personoplysninger inden for det strafferetlige område, jf. persondatalovens § 2, stk. 4, men bestemmelsen finder dog anvendelse i forbindelse med den grænseoverskridende udveksling af personoplysninger, jf. rammeafgørelsesbekendtgørelsens § 2, stk. 4.

Det fremgår af forarbejderne til persondataloven (Folketingstidende 1999-2000, tillæg A, s. 4092), at blokering af oplysninger indebærer, at det fortsat er tilladt at opbevare indsamlede oplysninger, hvorimod det ikke er tilladt at behandle og bruge oplysninger, herunder navnlig videregive dem til tredjemand. Oplysninger, som er blokeret, skal derfor være forsynet med en sådan markering, at en bruger informeres om blokeringen.

Det foreslås i *§ 17, stk. 3*, at den dataansvarlige i stedet for berigtigelse eller sletning efter de forslåede § 17, stk. 1 og 2, skal begrænse behandlingen af personoplysninger, hvis rigtigheden af personoplysningerne bestrides af den registrerede og deres rigtighed eller urigtighed ikke kan konstateres, eller personoplysningerne skal bevares som bevismiddel.

Med den foreslåede bestemmelse gives der mulighed for, at den dataansvarlige i stedet for berigtigelse eller sletning kan foretage begrænsning af anvendelsen af de pågældende oplysninger.

Der kan således ske begrænsning, hvis det ikke umiddelbart kan konstateres, om de personoplysninger, som den dataansvarlige myndighed har om den registrerede, er korrekte. Anvendelsen af oplysningerne vil i givet fald være begrænset, indtil den dataansvarlige har fundet ud af, om oplysningerne er korrekte. Hvis oplysningerne er korrekte, skal begrænsningen ophæves, jf. dog den foreslåede § 17, stk. 4.

Der kan endvidere ske begrænsning, hvis der er tale om oplysninger, der skal bevares som bevismidler. Det er f.eks. relevant i forhold til indholdet af et vidneudsagn, idet spørgsmålet om, hvorvidt de personoplysninger,

som fremgår af et vidneudsagn, er korrekte, skal håndteres i forbindelse med en straffesags behandling ved domstolene.

Begrænsning kan ske ved, at udvalgte oplysninger flyttes til et andet behandlingssystem, f.eks. til arkivformål, eller at udvalgte oplysninger gøres utilgængelige. I automatiske registre kan begrænsning ske ved hjælp af tekniske hjælpemidler. En begrænsning skal anføres i registeret på en sådan måde, at det tydeligt fremgår, at behandlingen af personoplysninger er begrænset, jf. herved direktivets præambelbetragtning nr. 47.

Der er således i praksis tale om en videreførelse af den forståelse af begrebet blokering, som følger af persondataloven.

Der henvises i øvrigt til pkt. 2.4.3.3 i lovforslagets almindelige bemærkninger.

Til stk. 4.

Det foreslås i *17, stk. 4*, at hvis behandling er begrænset som følge af, at rigtigheden af personoplysningerne bestrides af den registrerede, og deres rigtighed eller urigtighed ikke kan konstateres, skal den dataansvarlige underrette den registrerede herom, inden begrænsningen af behandling ophæves.

Den foreslåede bestemmelse skal ses i sammenhæng med den foreslåede § 17, stk. 3, idet der er tale om den situation, hvor der sker begrænsning som følge af, at det ikke umiddelbart kan konstateres, om de personoplysninger, som den dataansvarlige myndighed har om den registrerede, er korrekte. Anvendelsen af oplysningerne vil i givet fald være begrænset, indtil den dataansvarlige har fundet ud af, om oplysningerne er korrekte. Hvis oplysningerne er korrekte, skal begrænsningen ophæves.

Den foreslåede bestemmelse indebærer, at der i en sådan situation skal ske en forudgående underretning af den registrerede.

Der er ikke noget krav om, at den dataansvarlige myndighed afventer den registreredes svar på underretningen, inden begrænsningen ophæves. Bestemmelsen skal således ses i sammenhæng med den foreslåede *§ 17, stk. 5*.

Der henvises i øvrigt til pkt. 2.4.3.3 i lovforslagets almindelige bemærkninger.

Til stk. 5

Det foreslås i *§ 17, stk. 5*, at et afslag på en anmodning om berigtigelse, sletning eller begrænsning skal meddeles den registrerede skriftligt og skal være ledsaget af en begrundelse og en klagevejledning. Afgørelsen skal endvidere indeholde oplysninger om den registreredes ret til at lade den kompetente tilsynsmyndighed udøve den registreredes rettigheder i forhold til retten til berigtigelse, sletning eller begrænsning. Bestemmelsen i § 16, stk. 3, finder tilsvarende anvendelse.

Den foreslåede bestemmelse skal forstås i lyset af de almindelige regler i forvaltningslovens kapitler 6 og 7 om begrundelse og klagevejledning, idet det dog efter den foreslåede bestemmelse er obligatorisk for den dataansvarlige at give en skriftlig begrundelse, ligesom der er et særligt krav om at oplyse om muligheden for, at den registrerede kan udøve sine rettigheder i forhold til retten til berigtigelse, sletning eller begrænsning gennem tilsynsmyndigheden.

Til stk. 6

Det fremgår af persondatalovens § 37, stk. 2, at den dataansvarlige skal underrette den tredjemand, hvortil oplysningerne er videregivet, om, at de videregivne oplysninger er berigtiget, slettet eller blokeret i henhold til stk. 1, hvis en registreret person fremsætter anmodning herom. Dette gælder dog ikke, hvis underretningen viser sig umulig eller er uforholdsmæssigt vanskelig.

Bestemmelsen finder generelt ikke anvendelse for politiets, anklagemyndighedens og domstolenes behandling af personoplysninger inden for det strafferetlige område, jf. persondatalovens § 2, stk. 4, men bestemmelsen finder dog anvendelse i forbindelse med den grænseoverskridende udveksling af personoplysninger, jf. rammeafgørelsesbekendtgørelsens § 2, stk. 4.

Det foreslås i *17, stk. 6*, at den dataansvarlige skal underrette modtagere om, at der er sket berigtigelse, sletning eller begrænsning af personoplysninger. Modtagerne berigtiger eller sletter personoplysningerne eller begrænser behandling af personoplysninger, som de har ansvaret for.

Med den foreslåede bestemmelse sker der er skærpelse af forpligtelsen til at underrette modtagere om, at der er sket berigtigelse, sletning eller begrænsning af personoplysninger, som tillige udvides til at finde anvendelse i rent nationale forhold. Forpligtelsen skal dog ses i lyset af, at de kompetente myndigheder typisk videregiver oplysninger til en mere afgrænset kreds af modtagere.

Forpligtelsen for modtagerne til at berigtige, slette eller begrænse anvendelsen af de pågældende oplysninger gælder for de kompetente myndigheder. Forpligtelsen er således en understregning af det behandlingsprincip, som fremgår af den foreslåede § 4, stk. 4. . Det bemærkes i den forbindelse, at lovens definition af modtagere ikke omfatter dem, der modtager oplysninger i forbindelse med isolerede forespørgsler.

I det omfang, at der er tale om en behandling, herunder videregivelse, af oplysninger, som falder uden for det foreslåede anvendelsesområde for loven, reguleres spørgsmålet om retten til berigtigelse, sletning og begrænsning af persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen.

Til § 18

Til stk. 1

Det fremgår af persondatalovens § 31, at når en person fremsætter begæring om indsigt, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om, hvilke oplysninger der behandles, behandlingens formål, kategorierne af modtagere af oplysningerne og tilgængelig information om, hvorfra disse oplysninger stammer.

Det foreslås i *§ 18, stk. 1*, at oplysninger og meddelelser, der er nævnt i afsnit III, skal stilles til rådighed eller gives gratis i en kortfattet, letforståelig og lettilgængelig form og i et klart og enkelt sprog.

Med den foreslåede bestemmelse understreges det, at oplysninger efter den foreslåede § 13, stk. 1 og 2, meddelelser i forbindelse med den registreredes indsigtsanmodninger efter den foreslåede § 15 og eventuelle afslag herpå efter den foreslåede § 16 samt meddelelser om afslag på berigtigelse, sletning eller begrænsning af behandling efter den foreslåede § 17 skal

stilles til rådighed eller gives gratis og på en måde, som lettilgængelig og letforståelig for den almindelige borger.

Der henvises i øvrigt til pkt. 2.4.3.4 i lovforslagets almindelige bemærkninger.

Til stk. 2

Det fremgår af persondatalovens § 31, stk. 2, at den dataansvarlige snarest skal besvare indsigtsbegæringer som nævnt i § 31, stk. 1. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om, hvornår afgørelsen kan forventes at foreligge.

Det fremgår videre af persondatalovens § 34, at meddelelser i henhold til § 31, stk. 1, om den registreredes indsigtsret på begæring skal gives skriftligt. I tilfælde, hvor hensynet til den registrerede taler derfor, kan meddelelse dog gives i form af en mundtlig underretning om indholdet af oplysningerne.

Det foreslås i *§ 18, stk. 2*, at den dataansvarlige snarest og på skrift skal besvare begæringer som nævnt i afsnittet. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om hvornår anmodningen forventes besvaret.

Med den foreslåede bestemmelse gøres det obligatorisk for den dataansvarlige at besvare begæringer fra den registrerede. Den gældende ordning, hvorefter den registrerede skal underrettes, hvis begæringen ikke er besvaret inden for 4 uger, videreføres og udstrækkes til at omfatte alle de begæringer, som den registrerede kan fremsætte i medfør af bestemmelserne i afsnittet.

Der henvises i øvrigt til pkt. 2.4.3.3 i lovforslagets almindelige bemærkninger.

Til stk. 3

Retsplejelovens kapitel 66 indeholder regler om sigtede personers mv. adgang til materiale, som er tilvejebragt af politiet i forbindelse med strafferetlig forfølgning. Retsplejeloven indeholder endvidere regler om aktind-

sigt i domme, kendelser og andre dokumenter, der vedrører en straffesag. Udgangspunktet er, at enhver har ret til aktindsigt i domme og kendelser mv., ligesom den, der har en individuel, væsentlig interesse i et konkret retsspørgsmål, som udgangspunkt kan forlange at blive gjort bekendt med dokumenter, der vedrører en straffesag, herunder indførsler i retsbøgerne, i det omfang dokumenterne har betydning for vurderingen af det pågældende retsspørgsmål. Herudover indeholder retsplejeloven regler om berigtigelse af retsafgørelser.

Det foreslås i *stk. 3*, at når personoplysninger er indeholdt i en retsafgørelse eller et register, der er knyttet til udstedelsen af en retsafgørelse, skal anmodninger i medfør af dette afsnit gennemføres i henhold til retsplejelovens regler.

Retsplejelovens regler om adgangen til indsigt mv. i retsafgørelser indeholder de rettigheder, som fremgår af det foreslåede afsnit III.

Med den foreslåede bestemmelse sikres det således, at anmodninger om indsigt, berigtigelse, sletning eller begrænsning af behandling af personoplysninger håndteres efter retsplejelovens regler.

Til § 19

Det fremgår af persondatalovens § 33, at en registreret person, der har fået meddelelse efter § 31, stk. 1, om den registreredes indsigtsret ikke har krav på ny meddelelse før 6 måneder efter sidste meddelelse, medmindre der godtgøres en særlig interesse heri.

Det foreslås i *§ 19*, at den dataansvarlige kan afvise at imødekomme åbenbart grundløse eller overdrevent gentagne anmodninger, som er fremsat i henhold til bestemmelserne i dette afsnit.

Det er den dataansvarlige, som bærer bevisbyrden for, at betingelserne for, at der kan ske afvisning, er opfyldt. Det er således ikke op til den registrerede at godtgøre en berettiget interesse, men i det omfang, at den registrerede fremkommer med oplysninger om en sådan interesse, vil der formodningsvist ikke være grundlag for at afvise anmodningen i medfør af den foreslåede bestemmelse.

Til § 20

Til stk. 1

Det fremgår af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Det foreslås i *§ 20, stk. 1,* at den dataansvarlige skal gennemføre og om nødvendigt ajourføre og revidere de fornødne tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med loven. Hvis det står i rimeligt forhold til behandlingsaktiviteterne, skal den dataansvarlige tillige gennemføre de fornødne databeskyttelsespolitikker.

Med den foreslåede bestemmelse understreges den dataansvarliges forpligtelser. Forpligtelserne efter denne bestemmelse må imidlertid i praksis anses for at være dækket af den foreslåede § 27 om behandlingssikkerhed.

Der henvises i øvrigt til pkt. 2.5.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 2

Persondataloven indeholder ikke bestemmelser, som specifikt kræver databeskyttelse gennem design eller databeskyttelse gennem standardindstillinger.

Persondatalovens § 41, stk. 3, forpligter imidlertid den dataansvarlige og databehandleren til at beskytte mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven.

Persondataloven fastsætter ingen nærmere tidsmæssig ramme for, hvornår foranstaltningerne skal være truffet. Foranstaltningerne vil dog som udgangspunkt altid skulle forberedes eller implementeres forud for, at behandlingen påbegyndes. Datatilsynets praksis indeholder eksempler på, at persondatalovens behandlingsbetingelser og sikkerhedskrav skal iagttages ved indretningen af digitale løsninger.

Det foreslås i *§ 20, stk. 2*, at det præciseres, at foranstaltninger efter stk. 1 omfatter databeskyttelse gennem design og gennem standardindstillinger.

Et eksempel på, at der kan opnås databeskyttelse gennem design, er en teknisk foranstaltning, som pseudonymiserer personoplysningerne, dvs. at personoplysninger behandles på en sådan måde, at oplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger.

Pseudonymisering skal forstås som behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person, jf. direktivets artikel 3, nr. 5.

Pseudonymisering indebærer således, at enkelte direkte identificerende parametre, f.eks. navn eller personnummer, i oplysningerne erstattes med koder. Koderne opbevares på en særskilt liste, hvor man kan genfinde koblingen mellem oplysningerne og den person, som de vedrører.

Et eksempel på, at der kan opnås databeskyttelse gennem standardindstillinger, er indstillinger, som begrænser adgangen til de pågældende oplysninger eller fastsætter særlige opbevaringsperioder.

Kravet om databeskyttelse gennem design og standardindstillinger stiller ikke krav om, at eksisterende systemer skal redesignes. Kravene er således relevante i forhold til udvikling og design af fremtidige systemer.

Der henvises i øvrigt til pkt. 2.5.3.1 i lovforslagets almindelige bemærkninger.

Til § 21

Spørgsmålet om fælles dataansvarlige er ikke direkte reguleret i persondataloven. Det følger imidlertid af definitionen af begrebet ”den dataansvarlige” i persondatalovens § 3, nr. 4, at dette kan være en fysisk eller juridisk person, offentlig myndighed, institution eller ethvert andet organ, der alene

eller *sammen med andre* afgør, til hvilket formål og med hvilke virkemidler der må foretages behandling af oplysninger.

Spørgsmålet om fordelingen af ansvar og forpligtelser for de fælles dataansvarlige er ikke reguleret direkte i gældende ret. I sager, hvor Datatilsynet har accepteret et fælles dataansvar, har tilsynet lagt til grund, at der skal foreligge klare retningslinjer og instruktionsbeføjelser for så vidt angår behandlingen af oplysninger. Herudover skal de registrerede kunne gøre deres rettigheder efter persondatalovens kapitel III, såsom retten til indsigt, oplysninger mv., gældende over for enhver af de fælles dataansvarlige.

Ordningerne med fælles dataansvarlige forekommer imidlertid forholdsvis sjældent i praksis. Fælles dataansvarlige har dog været anvendt inden for politiet, der bl.a. er kendetegnet ved anvendelsen af en række fælles centrale it-systemer, der understøtter udveksling af oplysninger på tværs af flere dataansvarlige myndigheder.

Det foreslås i *§ 21*, at flere dataansvarlige i fællesskab kan fastsætte formålene med og hjælpemidlerne til behandling. De dataansvarlige skal om nødvendigt fastsætte en ordning for en fordeling af ansvaret for, at behandlingen er i overensstemmelse med loven, herunder navnlig i forhold til den registreredes rettigheder efter kapitel 5-7. Ordningen skal tillige indeholde oplysninger om et fælles kontaktpunkt for de dataansvarlige eller om kontaktpunkterne for de enkelte dataansvarlige.

Med den foreslåede bestemmelse indføres der således eksplicitte regler om fælles dataansvarlige.

Bestemmelsen vil bl.a. kunne anvendes inden for politiets samlede virksomhed med henblik på at gennemføre en ensartet, omkostningseffektiv og – navnlig for den registrerede – tilgængelig regulering af flere fælles dataansvarliges indbyrdes forhold og varetagelse af kontakten til registrerede.

En ordning med fælles dataansvarlige vil i øvrigt ligeledes kunne understøtte en generel og ensartet beskrivelse af de pågældende myndigheders it-systemer, behandlingsaktiviteter, efterlevelsen af anden relevant databeskyttelsesretlig regulering og i den forbindelse understøtte de dataansvarliges generelle efterlevelse af loven gennem iagttagelse af princippet om ansvarlighed.

Kravet om, at de fælles dataansvarlige skal udpege et kontaktpunkt, kan opfyldes ved at udpege den eller de dataansvarliges databeskyttelsesrådgiver som kontaktpunkt.

Der henvises i øvrigt til pkt. 2.5.3.2 i lovforslagets almindelige bemærkninger.

Til § 22

Til stk. 1

Det fremgår af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Det fremgår videre af persondatalovens § 42, stk. 1, at når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.

Det foreslås i *§ 22, stk. 1*, at når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 20 og § 24 nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.

Med den foreslåede bestemmelse sker der en videreførelse af reglerne om den dataansvarliges forpligtelse til at sikre, at databehandleren kan træffe de nødvendige foranstaltninger.

Der henvises i øvrigt til pkt. 2.5.3.3 i lovforslagets almindelige bemærkninger.

Til stk. 2

Det fremgår af persondatalovens § 42, stk. 2, at gennemførelse af en behandling ved en databehandler skal ske i henhold til en skriftlig aftale parterne imellem. Af aftalen skal det fremgå, at databehandleren alene handler

efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren. Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne.

Hvis en databehandler foretager behandling af oplysninger, uden at der foreligger en instruks fra den dataansvarlige – dvs. databehandleren fastlægger formålene med og hjælpemidlerne til behandling – anses denne databehandler for at være en dataansvarlig, for så vidt angår den pågældende behandling. Dette vil navnlig indebære, at behandlingen alene vil være lovlig i det omfang den pågældende – nye – dataansvarlige kan påvise et lovligt grundlag for behandlingen af de pågældende personoplysninger. Herudover må der i et sådanne tilfælde oftest forventes også at foreligge en overtrædelse af databehandleraftalen.

Såfremt en behandling i videre omfang end instrueret af den dataansvarlige følger af anden lovgivning, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige forud for, at den pågældende behandling foretages.

Det foreslås i *§ 22, stk. 2*, at gennemførelse af en behandling ved en databehandler skal ske i henhold til lov eller en skriftlig aftale mellem databehandleren og den dataansvarlige. Loven eller aftalen skal fastsætte genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder. Det skal navnlig fremgå, at databehandleren:

1) kun må handle efter instruks fra den dataansvarlige,
2) sikrer, at de fysiske personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt,
3) bistår den dataansvarlige på enhver hensigtsmæssig måde med at sikre overholdelse af bestemmelserne om den registreredes rettigheder,
4) efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysningerne til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, medmindre anden lovgivning foreskriver opbevaring af personoplysningerne,

5) stiller alle oplysninger, der er nødvendige for at påvise overholdelse af denne bestemmelse, til rådighed for den dataansvarlige, og
6) overholder betingelserne i stk. 2 og 3 med henblik på at gøre brug af en anden databehandler.

Med den foreslåede bestemmelse fastsættes der detaljerede krav til indholdet i en databehandleraftale, og dermed til databehandlerens forpligtelser over for den dataansvarlige, end efter gældende ret.

Bestemmelsen indebærer, at pligten til at sikre, at en databehandling finder sted i overensstemmelse med de oplistede krav gælder både for den dataansvarlige og eventuelle databehandlere og underdatabehandlere.

Det fremgår endvidere af bestemmelsen, at en databehandler senest 14 dage forud for, at der sker overladelse af behandling til en underdatabehandler i medfør af en generel aftale med den dataansvarlige herom, skal underrette den dataansvarlige om overladelsen. Den dataansvarlige vil i den forbindelse kunne modsætte sig overladelsen, hvis det anses for nødvendigt.

De kompetente myndigheder vil tillige behandle personoplysninger i sager og med formål, som falder uden for det foreslåede anvendelsesområde for loven. Denne behandling vil i stedet være omfattet af persondataloven og – fra den 25. maj 2018 – databeskyttelsesforordningen. Dette indebærer, at eventuelle databehandleraftaler vil skulle overholde kravene i såvel retshåndhævelsesdirektivet som – efter den 25. maj 2018 – databeskyttelsesforordningen.

Der henvises i øvrigt til pkt. 2.5.3.3 i lovforslagets almindelige bemærkninger.

Til stk. 3

Det fremgår af persondatalovens § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Loven indeholder således ikke en eksplicit regulering af den situation, hvor en databehandler ønsker at gøre brug af en underdatabehandler.

Det foreslås i *stk. 3*, at en databehandlers overladelse af behandling til en anden databehandler skal ske i henhold til en generel eller specifik skriftlig aftale med den dataansvarlige. Sker overladelse i henhold til en generel aftale, skal databehandleren underrette den dataansvarlige herom senest 14 dage forud for overladelsen.

Med den foreslåede bestemmelse sker der en præcisering af kravet om, at en databehandler alene må behandle oplysninger efter instruks fra den dataansvarlige.

Kravet om, at databehandleren senest 14 dage forud for overladelsen skal underrette den dataansvarlige om, at der sker overladelse af behandling til en underdatabehandler i medfør af en generel aftale, har til formål at sikre, at den dataansvarlige har mulighed for at sikre sig, at også underdatabehandleren træffer de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger, jf. herved den dataansvarliges forpligtelser efter den foreslåede § 22, stk. 1.

Der henvises i øvrigt til pkt. 2.5.3.3 i lovforslagets almindelige bemærkninger.

Til stk. 4

Det fremgår af persondatalovens § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Det foreslås i *§ 22, stk. 4*, at enhver, der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, kun må behandle disse oplysninger efter instruks fra den dataansvarlige, medmindre det følger af anden lovgivning, at den pågældende skal foretage behandlingen.

Med den foreslåede bestemmelse sker der en videreførelse af persondatalovens regler om, at behandling af oplysninger skal ske på baggrund af en instruks fra den dataansvarlige.

Der henvises i øvrigt til pkt. 2.5.3.3 i lovforslagets almindelige bemærkninger.

Til § 23

Persondataloven indeholder ikke krav om, at den dataansvarlige eller databehandleren skal føre fortegnelser over behandlingsaktiviteter.

Persondatalovens kapitel 12 (§§ 43-47) indeholder dog regler om anmeldelse af behandlinger, der foretages for den offentlige forvaltning, til tilsynsmyndigheden.

Det fremgår således af lovens § 43, jf. § 44, at der skal ske anmeldelse til tilsynsmyndigheden forinden iværksættelse af behandling af fortrolige oplysninger. Anmeldelsen skal indeholde en række nærmere angivne oplysninger, herunder om behandlingens formål, en generel beskrivelse af behandlingen, kategorierne af registrerede og foranstaltninger, der iværksættes af hensyn til behandlingssikkerheden og oplysninger om tidspunktet for sletning af oplysningerne.

Persondatalovens § 54 indeholder regler om, at tilsynsmyndigheden skal føre en fortegnelse over de modtagne anmeldelser, og at denne fortegnelse skal indeholde de samme oplysninger som anmeldelsen. Den dataansvarlige skal stille disse oplysninger til rådighed for enhver, der anmoder herom, jf. bestemmelsens stk.2.

Det foreslås i *§ 23, stk. 1*, at dataansvarlige forpligtes til at føre skriftlige fortegnelser over alle kategorier af behandlingsaktiviteter under deres ansvar. Fortegnelserne skal indeholde følgende oplysninger:

1) navn på og kontaktoplysninger for den dataansvarlige og, hvis det er relevant, den fælles dataansvarlige og databeskyttelsesrådgiveren,
2) formålene med behandlingen,
3) de kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, herunder modtagere i tredjelande eller internationale organisationer,
4) en beskrivelse af kategorierne af registrerede og kategorierne af personoplysninger,
5) hvor det er relevant, brugen af profilering,

6) hvor det er relevant, kategorierne af overførsler af personoplysninger til et tredjeland eller en international organisation,
7) en angivelse af retsgrundlaget for behandlingsaktiviteten, herunder overførsler, hvortil personoplysningerne er bestemt,
8) hvis det er muligt, de forventede tidsfrister for sletning af de forskellige kategorier af personoplysninger, og
9) hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i § 27.

Det foreslås endvidere i *§ 23, stk. 2*, at databehandleren forpligtes til at føre skriftlige fortegnelser over alle kategorier af behandlingsaktiviteter, der foretages på vegne af en dataansvarlig. Fortegnelserne skal indeholde følgende oplysninger:

1) navn på og kontaktoplysninger for databehandleren eller databehandlerne, for hver dataansvarlig, på hvis vegne databehandleren handler, samt, hvis det er relevant, databeskyttelsesrådgiveren,
2) de kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige,
3) hvor det er relevant, overførsler af personoplysninger til et tredjeland eller en international organisation, når den dataansvarlige udtrykkeligt har givet instruks herom, herunder angivelse af dette tredjeland eller denne internationale organisation, og
4) hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i § 27.

Den dataansvarlige og databehandleren skal ikke føre fortegnelsen i en bestemt form, andet end kravet om, at fortegnelsen skal foreligge skriftligt og elektronisk, skal opfyldes. Der er således intet til hinder for, at en fortegnelse føres i f.eks. et skema eller i et almindeligt tekstbehandlingsdokument, der let kan printes og stilles til rådighed for tilsynsmyndigheden, såfremt denne anmoder herom.

Der henvises i øvrigt til pkt. 2.5.3.5 i lovforslagets almindelige bemærkninger.

Til § 24

Det fremgår således af § 19, jf. § 2, stk. 2, i sikkerhedsbekendtgørelsen, at der skal foretages maskinel registrering (logning) af alle anvendelser af fortrolige personoplysninger. Registreringen skal mindst indeholde oplys-

ning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Det fremgår videre af bestemmelsens stk. 2, at stk. 1 ikke finder anvendelse for personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form. Det samme gælder sådanne dokumenter, som foreligger i endelig form, hvis der sker sletning inden for en af den dataansvarlige myndighed nærmere fastsat kortere frist.

Bestemmelsen i stk. 1 finder heller ikke anvendelse, hvis behandlingen af personoplysninger udelukkende sker ved afvikling af programmer, som foretager en forud defineret massebehandling af personoplysninger (batchkørsler). Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen, jf. stk. 3.

Bestemmelsen i stk. 1 finder endvidere ikke anvendelse, hvis behandlingen af personoplysningerne udelukkende sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med et kodenummer eller lignende. Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen, jf. stk. 4.

Bestemmelsen i stk. 1 finder endelig ikke anvendelse for personoplysninger, som i form af måle- eller analyseresultater automatisk lagres i medicoteknisk udstyr. Undtagelsen omfatter tillige personoplysninger, som manuelt registreres i medicoteknisk udstyr til supplering af automatisk lagrede oplysninger, jf. stk. 5.

Sikkerhedsbekendtgørelsen for domstolene indeholder i § 19 regler svarende til de ovennævnte regler i sikkerhedsbekendtgørelsens § 19, stk. 1, 2 og 4.

Rammeafgørelsesbekendtgørelsens § 10 indeholder et krav om, at den dataansvarlige med henblik på at kontrollere, om databehandlingen er lovlig, samt med henblik på at udøve egenkontrol og sikre integritet og sikkerhed skal registrere eller dokumentere hver videregivelse af personoplysninger.

Registreringen eller dokumentationen skal bl.a. indeholde oplysninger om, til hvilke organer der er blevet eller kan være blevet videregivet eller stillet

personoplysninger til rådighed ved hjælp af datakommunikationsudstyr, og hvilke personoplysninger der er indlæst i edb-systemerne, hvornår og af hvem.

Registreringer, der foretages, eller dokumentation, der udarbejdes, videregives til Datatilsynet på dennes anmodning med henblik på kontrol af databeskyttelsen. For domstolenes vedkommende sker videregivelsen til Domstolsstyrelsen. Datatilsynet og Domstolsstyrelsen anvender kun disse oplysninger med henblik på kontrol af databeskyttelsen og med henblik på at sikre en korrekt databehandling og dataenes integritet og sikkerhed, jf. § 10, stk. 2.

Det foreslås i *stk. 1*, at der i automatiske databehandlingssystemer skal foretages logning af indsamling, ændring, søgning, videregivelse, herunder overførsel, samkøring og sletning.

Med den foreslåede bestemmelse sker der en implementering af retshåndhævelsesdirektivets artikel 25. Som anført oven for i pkt. 2.5.3.4 giver det det nærmere omfang af direktivets forpligtelse til at foretage logning imidlertid anledning til tvivl, herunder i forhold til spørgsmålet om, i hvilket omfang det i øvrigt vil være muligt at opretholde den gældende ordning for logning i sikkerhedsbekendtgørelserne.

Det foreslås på den baggrund videre i *stk. 2*, at justitsministeren får bemyndigelse til at fastsætte nærmere regler om, hvilke automatiske databehandlingssystemer logningskravet skal finde anvendelse på.

Denne ordning giver mulighed for, at der sammen med de kompetente myndigheder kan ske en nærmere afklaring af rækkevidden af logningsforpligtelsen, inden der tages initiativ til at ændre de kompetente myndigheders automatiske databehandlingssystemer.

Det sikres endvidere herved, at der vil kunne ske en løbende indfasning af forpligtelsen, eventuelt i forbindelse med at der sker udskiftning af eksisterende automatiske behandlingssystemer.

Logningskravet vil dog skulle finde anvendelse for alle relevante automatiske databehandlingssystemer senest den 6. maj 2023 eller, hvis det måtte vise sig, at direktivets logningskrav medfører alvorlige vanskeligheder for driften af de kompetente myndigheders automatiske behandlingssystemer, senest den 6. maj 2026.

Der henvises i øvrigt til pkt. 2.5.3.4 i lovforslagets almindelige bemærkninger.

Til § 25

Gældende ret indeholder ikke et krav om, at den dataansvarlige skal udarbejde konsekvensanalyser.

Det foreslås i *§ 25, stk. 1*, at hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder, skal den dataansvarlige forud for behandlingen foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger.

Angivelsen af, at konsekvensanalysen skal foretages forud for behandlingen, indebærer, at kravet alene er relevant i forhold til behandling, der foretages den 1. maj 2017 eller senere, dvs. efter det foreslåede ikrafttrædelsestidspunkt. Der skal med andre ord ikke foretages konsekvensanalyser af eksisterende behandlingsaktiviteter, jf. også den foreslåede § 53 og bemærkningerne hertil.

Det foreslås videre i *§ 25, stk. 2*, at analysen skal indeholde en generel beskrivelse af de planlagte behandlingsaktiviteter, en vurdering af risiciene for de registreredes rettigheder, de foranstaltninger, der påtænkes for at imødegå disse risici, garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af denne lov, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

De krævede oplysninger er i vidt omfang sammenfaldende med de oplysninger, som en anmeldelse efter persondatalovens kapitel V skal indeholde, jf. persondatalovens § 43, stk. 2.

Der henvises i øvrigt til pkt. 2.5.3.5 i lovforslagets almindelige bemærkninger.

Til § 26

Gældende ret indeholder ikke et krav om, at den dataansvarlige skal foretage forudgående høring af tilsynsmyndigheden.

Persondatalovens kapitel 12 (§§ 43-47) indeholder dog regler om anmeldelse af behandlinger, der foretages for den offentlige forvaltning, til tilsynsmyndigheden.

Det fremgår således af lovens § 43, jf. § 44, at der skal ske anmeldelse til tilsynsmyndigheden forinden iværksættelse af behandling af fortrolige oplysninger. Anmeldelsen skal indeholde en række nærmere angivne oplysninger, herunder om behandlingens formål, en generel beskrivelse af behandlingen, kategorierne af registrerede og foranstaltninger, der iværksættes af hensyn til behandlingssikkerheden og oplysninger om tidspunktet for sletning af oplysningerne.

I visse situationer skal der tillige indhentes en udtalelse fra tilsynsmyndigheden, jf. lovens § 45. Der er tale om bl.a. behandlinger, som omfatter følsomme oplysninger eller oplysninger om rent private forhold, og behandlinger, som udelukkende finder sted i videnskabeligt eller statistisk øjemed.

Det foreslås i *§ 26, stk. 1*, at den dataansvarlige eller databehandleren skal høre tilsynsmyndigheden inden behandling af personoplysninger, der vil indgå som en del af et nyt register, der skal oprettes, når:

1) en konsekvensanalyse vedrørende databeskyttelse, jf. den foreslåede § 25, viser, at behandlingen vil føre til en høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen, eller
2) den type behandling, navnlig ved brug af nye teknologier, mekanismer eller procedurer, indebærer en høj risiko for de registreredes rettigheder.

Pligten til forudgående høring af tilsynsmyndigheden knytter sig til behandling af personoplysninger i *nye registre*. Der skal således ikke foretages forudgående høring, hvis der iværksættes en ny behandling i et allerede eksisterende register.

Den forudgående høring i medfør af *stk. 1, nr. 1*, har til formål at give tilsynsmyndigheden mulighed for at vurdere, om de foranstaltninger, som den dataansvarlige vil træffe for at begrænse risikoen, er tilstrækkelige.

Den forudgående høring i medfør af *stk. 1, nr. 2*, kan være relevant, hvis der er tale om nye registre, som behandler oplysninger om et meget stort antal registrerede, eller særlige kategorier af oplysninger, jf. den foreslåede § 10.

Kravet om forudgående høring vil i praksis ofte være sammenfaldende med de situationer, hvor der efter gældende ret skal ske anmeldelse til tilsynsmyndigheden.

Kravet om forudgående høring finder anvendelse på registre, der oprettes den 1. maj 2017 eller senere, dvs. efter det foreslåede ikrafttrædelsestidspunkt. Der skal med andre ord ikke foretages høring af tilsynsmyndigheden i forhold til eksisterende registre, jf. også den foreslåede § 53 og bemærkningerne hertil.

Det foreslås videre i *§ 26, stk. 2*, at hvis tilsynsmyndigheden finder, at den planlagte behandling ikke vil overholde loven, herunder navnlig hvis den dataansvarlige ikke tilstrækkeligt har identificeret eller begrænset risikoen, giver tilsynsmyndigheden inden for en periode på op til 6 uger efter modtagelse af anmodningen om høring den dataansvarlige og, hvor det er relevant, databehandleren skriftlig rådgivning. Tilsynsmyndigheden kan i den forbindelse anvende enhver af sine beføjelser, jf. kapitel 20. Denne periode kan forlænges med en måned 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.

Med den foreslåede bestemmelse reguleres tilsynsmyndighedens reaktionsmuligheder i forhold til en forudgående høring.

Det foreslås endeligt i § 26, stk. 3, at tilsynsmyndighederne skal kunne fastsætte en liste over de behandlingsaktiviteter, hvor der i henhold til stk. 1 skal foretages en forudgående høring.

Med den foreslåede bestemmelse gives tilsynsmyndigheden en adgang til at fastsætte en liste over de behandlingsaktiviteter, hvor der skal ske en forudgående høring. Der skal være tale om behandlingsaktiviteter i et *nyt* register, jf. den foreslåede § 26, stk. 1.

Der henvises i øvrigt til pkt. 2.5.3.5 i lovforslagets almindelige bemærkninger.

Til § 27

Det fremgår af persondatalovens § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Efter persondatalovens § 41, stk. 3, skal den dataansvarlige træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Efter persondatalovens § 41, stk. 4, skal der for oplysninger, der behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold (krigsreglen).

Persondatalovens § 41, stk. 5, bemyndiger justitsministeren til at fastsætte nærmere regler om de i stk. 3 anførte sikkerhedsforanstaltninger. Justitsministeren har med hjemmel i bestemmelsen udstedt sikkerhedsbekendtgørelsen og sikkerhedsbekendtgørelsen for domstolene.

Det fremgår af bekendtgørelsernes § 5, at den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af bekendtgørelsen. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinier for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.

De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i myndigheden, jf. bestemmelsernes stk. 2.

Bekendtgørelserne indeholder herudover nærmere regler om bl.a. instruktion over for medarbejdere, der behandler personoplysninger, samt om autorisation og adgangskontrol.

Det foreslås i *stk. 1*, at den dataansvarlige og databehandleren under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og behandlingens karakter, omfang, sammenhæng og formål samt risicienes varierende sandsynlighed og alvor for fysiske personers rettigheder skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, navnlig for så vidt angår behandlingen af de særlige kategorier af personoplysninger, der er omfattet af den foreslåede § 10.

Med den foreslåede bestemmelse fastslås det generelle princip om, at de fornødne tekniske og organisatoriske foranstaltninger skal fastsættes ud fra en risikobaseret tilgang.

Dette princip er i praksis en videreførelse af det gældende krav i persondatalovens § 41, stk. 3.

Det foreslås videre i *stk. 2*, at for så vidt angår automatisk behandling, skal den dataansvarlige eller databehandleren på grundlag af en risikovurdering gennemføre foranstaltninger til at sikre, at:

1) uautoriserede personer ikke kan få adgang til det behandlingsudstyr, der benyttes til behandling (kontrol med fysisk adgang til udstyret),
2) der ikke sker uautoriseret læsning, kopiering, ændring eller sletning af datamedier (kontrol med datamedier),
3) der ikke sker uautoriseret indlæsning af personoplysninger samt uautoriseret læsning, ændring eller sletning af opbevarede personoplysninger (kontrol med opbevaring),
4) automatiske behandlingssystemer ikke via datakommunikationsudstyr kan benyttes af uautoriserede personer (brugerkontrol),
5) personer med bemyndigelse til at anvende et automatisk behandlingssystem kun har adgang til de personoplysninger, der

er omfattet af deres adgangstilladelse (kontrol med dataadgangen),

6) det er muligt at kontrollere og fastslå de modtagere, til hvilke der er blevet eller kan transmitteres eller stilles oplysninger til rådighed ved hjælp af datakommunikationsudstyr (kommunikationskontrol),
7) det er muligt efterfølgende at undersøge og fastslå, hvilke personoplysninger der er indlæst i automatiske behandlingssystemer, og hvornår og af hvem personoplysningerne blev indlæst (kontrol med indlæsning),
8) der ikke sker uautoriseret læsning, kopiering, ændring eller sletning af personoplysninger i forbindelse med overførsler af disse eller under transport af datamedier (transportkontrol), og
9) de anvendte systemer i tilfælde af teknisk uheld kan genetableres (genopretning), og
10) systemet fungerer, at indtrufne fejl meldes (pålidelighed), og at opbevarede personoplysninger ikke bliver ødelagt som følge af fejlfunktioner i systemet (integritet).

Der sker med den foreslåede bestemmelse en detaljeret oplistning af de sikkerhedskrav, som stilles ved automatisk behandling af personoplysninger. Kravene er i vidt omfang en videreførelse af de gældende regler om behandlingssikkerhed i persondatalovens § 41 og sikkerhedsbekendtgørelsens regler. Kravene i de foreslåede nr. 6 og 7 skal ses i lyset af den foreslåede § 24 om logning.

Det foreslås videre i *stk. 3*, at for oplysninger af særlig interesse for fremmede magter skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Med den foreslåede bestemmelse sker der en videreførelse af den såkaldte krigsregel, som indebærer, at der skal træffes særlige foranstaltninger i forhold til oplysninger med særlig interesse for fremmede magter bl.a. for dermed hurtigt og effektivt at kunne overtage den almindelige administration.

Den foreslåede bestemmelse indebærer, at ikke alle behandlinger vil kunne udføres af en databehandler i udlandet, hvis en sådan overladelse medfører, at krigsreglen ikke kan iagttages af den dataansvarlige.

Bestemmelsen varetager hensynet til den offentlige sikkerhed og skal fortolkes i lyset af Danmarks EU-retlige forpligtelser.

Der foreslås videre i *stk. 4*, at justitsministeren bemyndiges til at fastsætte nærmere regler om sikkerhedsforanstaltninger. Der er tale om en videreførelse af den gældende bestemmelse i persondatalovens § 41, stk. 5.

Det foreslås endeligt i *stk. 5*, at justitsministeren efter indstilling fra en kompetent myndighed kan fastsætte regler om, at det er ufornødent, at personoplysninger omfattet af stk. 3, underlægges foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse, hvis dette ud fra en samlet vurdering må anses for forsvarligt.

Med den foreslåede bestemmelse sikres det som noget nyt, at justitsministeren efter indstilling fra en kompetent myndighed kan fastsætte nærmere regler om, at oplysninger, der er omfattet af den forslåede bestemmelse i § 27, stk. 3, ikke skal være underlagt et krav om, at det i tilfælde af krig eller lignende forhold skal være muligt at foretage bortskaffelse eller tilintetgørelse.

Krigsreglen indebærer som nævnt ovenfor, at visse registre – som følge af karakteren af de personoplysninger, som er indeholdt heri – skal føres i Danmark.

Den foreslåede bestemmelse vil gøre det praktisk muligt for de kompetente myndigheder helt eller delvist at gøre brug af f.eks. cloud-tjenester, hvor opbevaringen af oplysninger sker på servere i udlandet.

Vurderingen af, om det kan anses for forsvarligt at opbevare de pågældende oplysninger i udlandet, vil navnlig inddrage de pågældende oplysningers karakter og de tekniske og organisatoriske foranstaltninger, jf. § 27, stk. 2, som træder i stedet for de foranstaltninger, som ellers skulle have været truffet i medfør af den foreslåede § 27, stk. 3.

Der henvises i øvrigt til pkt. 2.6.3.1 i lovforslagets almindelige bemærkninger.

Til § 28

Til stk. 1

Persondataloven indeholder ikke regler, hvorefter dataansvarlige, der har sikkerhedsbrud i forbindelse med behandling af personoplysninger, har pligt til at underrette tilsynsmyndigheden herom.

Det foreslås i *§ 28, stk. 1*, at ved brud på persondatasikkerheden skal den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet, anmelde bruddet til tilsynsmyndigheden, medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder. En overskridelse af fristen på 72 timer skal begrundes.

Med den foreslåede bestemmelse forpligtes den dataansvarlige til i visse situationer at anmelde brud på datasikkerheden til tilsynsmyndigheden.

Der skal ikke ske anmeldelse, hvis det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder. Der kunne f.eks. være tale om en situation, hvor en dataansvarlig har mistet et bærbart medie, hvorpå der er lagret persondata i krypteret form. Der kan være anvendt en tilstrækkelig stærk kryptering, som ikke kan brydes eller omgås inden for en tilstrækkelig lang årrække, og uvedkommende har ikke og får ikke mulighed for at dekryptere data på normal vis – f.eks. ved at komme i besiddelse af rette krypteringsnøgle.

Bevisbyrden for, at det var usandsynligt, at bruddet ville indebære en risiko for fysiske personers rettigheder påhviler den dataansvarlige. Rettigheder skal forstås i bred forstand og retter sig således ikke kun til den registreredes rettigheder i medfør af nærværende lov.

Der henvises i øvrigt til pkt. 2.6.3.2 i lovforslagets almindelige bemærkninger.

Til stk. 2

Det foreslås i *§ 28, stk. 2*, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om et brud på persondatasikkerheden.

Med den foreslåede bestemmelse sikres det, at den dataansvarlige bliver bekendt med eventuelle sikkerhedsbrud. Den dataansvarlige skal på baggrund af underretningen fra databehandleren vurdere, om der skal ske anmeldelse til tilsynsmyndigheden efter den foreslåede § 28, stk. 1.

Der henvises i øvrigt til pkt. 2.6.3.2 i lovforslagets almindelige bemærkninger.

Til stk. 3 og 4

Det foreslås i *§ 28, stk. 3,* at anmeldelsen efter stk. 1 skal:

1) beskrive karakteren af bruddet på persondatasikkerheden, herunder i videst muligt omfang kategorierne og det berørte antal registrerede samt kategorierne og det berørte antal registreringer af personoplysninger,
2) angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes,
3) beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden, og
4) 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.

Det foreslås videre i § *28, stk. 4*, at når det ikke er muligt at forelægge oplysningerne, der er nævnt i stk. 3, samlet for tilsynsmyndigheden, skal oplysningerne meddeles trinvis uden unødig forsinkelse.

Med de foreslåede bestemmelser fastslås det, hvilke oplysninger anmeldelsen til tilsynsmyndigheden skal indeholde, og at det ikke er nødvendigt for den dataansvarlige at indsamle alle oplysningerne, inden anmeldelsen sendes til tilsynsmyndigheden.

Der henvises i øvrigt til pkt. 2.6.3.2 i lovforslagets almindelige bemærkninger.

Til stk. 5

Det foreslås i *§ 28, stk. 5*, at den dataansvarlige skal dokumentere alle brud på persondatasikkerheden, som er omfattet af stk. 1, herunder de faktiske omstændigheder vedrørende bruddet, dets virkninger og de trufne afhjælpende foranstaltninger.

Med den foreslåede bestemmelse forpligtes den dataansvarlige til at opbevare de oplysninger, som i øvrigt skal fremgå af anmeldelsen til tilsynsmyndigheden.

Der henvises i øvrigt til pkt. 2.6.3.2 i lovforslagets almindelige bemærkninger.

Til stk. 6

Det foreslås i *§ 28, stk. 6*, at hvis bruddet på persondatasikkerheden omhandler oplysninger, der er transmitteret af eller til en dataansvarlig i en anden medlemsstat, skal oplysninger, der er nævnt i stk. 3, uden unødig forsinkelse meddeles til den dataansvarlige i denne medlemsstat.

Med den foreslåede bestemmelse forpligtes den dataansvarlige til at underrette dataansvarlige i andre medlemsstater, hvis der er tale om oplysninger, som er modtaget fra eller videregivet til en anden medlemsstat. Det sikres herved, at den udenlandske dataansvarlige kan tage højde for, at der f.eks. er sket en utilsigtet spredning af oplysningerne, hvilket kan have betydning for f.eks. en verserende efterforskning af et strafbart forhold.

Der henvises i øvrigt til pkt. 2.6.3.2 i lovforslagets almindelige bemærkninger.

Til § 29

Persondataloven indeholder ikke eksplicitte regler, hvorefter dataansvarlige, der har sikkerhedsbrud i forbindelse med behandling af personoplysninger, har pligt til at underrette de registrerede herom.

Persondatalovens § 5, stk. 1, indeholder imidlertid et krav om, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik.

God databehandlingsskik anses efter praksis fra Datatilsynet for bl.a. at omfatte krav til den dataansvarlige om at foretage underretning af berørte personer ved brud på datasikkerheden, når personoplysninger er kommet til uvedkommendes kendskab eller har været i risiko herfor. Ved vurderingen af spørgsmålet om underretning må den dataansvarlige bl.a. tage oplysningernes karakter og de mulige konsekvenser for de berørte i betragtning. Ved utilsigtet offentliggørelse af personoplysninger på en hjemme-

side på internettet skal de dataansvarlige således bl.a. foretage underretning af de berørte personer.

Det foreslås i *§ 29, stk. 1*, at ved brud på persondatasikkerheden, som sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder, skal den dataansvarlige uden unødig forsinkelse underrette den registrerede om bruddet.

Med den foreslåede bestemmelse forpligtes den dataansvarlige til i visse situationer at underrette den registrerede om brud på datasikkerheden.

I modsætning til kravet om anmeldelse af et brud på persondatasikkerheden til tilsynsmyndigheden, jf. den foreslåede § 28, skal underretningen skal ske *uden unødig forsinkelse*, efter at bruddet er påvist. Underretningen skal give den registrerede mulighed for at træffe de fornødne forholdsregler. Det er således væsentligt, at der sker en hurtig underretning, hvis bruddet på datasikkerheden kan have store konsekvenser for den registrerede, f.eks. hvis adresseoplysninger mv. for et vidne i en straffesag, bliver tilgængelige for tredjemand.

Det foreslås videre i *§ 29, stk. 2*, at underretningen i et klart og enkelt sprog skal beskrive karakteren af bruddet samt indeholde de oplysninger, der er nævnt i § 28, stk. 3, nr. 2-4.

Det foreslås herudover i *§ 29, stk. 3*, at kravet om underretning ikke gælder, hvis:

1) 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 f.eks. på grund af kryptering gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil,
2) den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder som omhandlet i stk. 1 sandsynligvis ikke længere er reel, eller
3) det vil kræve en uforholdsmæssig indsats af den dataansvarlige. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

Med den foreslåede bestemmelse sker der en nærmere regulering af, hvornår der ikke skal gives en underretning til den registrerede. Bestemmelsen skal ses som en præcisering af den risikovurdering, som den dataansvarlige skal foretage i medfør af den foreslåede § 29, stk. 1.

Der vil f.eks. kunne undlades at foretage underretning efter *nr. 1*, hvis der er tale om en situation, hvor en dataansvarlig har mistet et bærbart medie, hvorpå der er lagret persondata, men hvor der er anvendt en tilstrækkelig stærk kryptering, som indebærer, at uvedkommende ikke kan få adgang til indholdet.

Der vil f.eks. kunne undlades at foretage underretning efter nr. 2, hvis der er tale om en situation, hvor der i en periode har været risiko for ikke-autoriseret adgang til personoplysninger, men den dataansvarlige sørger for, at adgangen hindres, og den dataansvarliges log viser, at der rent faktisk ikke har været uautoriserede personer, som har tilgået oplysningerne.

Det foreslås desuden i *§ 29, stk. 4*, at hvis den dataansvarlige ikke allerede har underrettet den registrerede om bruddet på persondatasikkerheden, kan tilsynsmyndigheden efter at have overvejet sandsynligheden for, at bruddet på persondatasikkerheden indebærer en høj risiko, kræve, at den dataansvarlige gør dette, eller beslutte, at en af betingelserne i den foreslåede § 29, stk. 3, er opfyldt.

Med den foreslåede bestemmelse får tilsynsmyndigheden mulighed for at pålægge den dataansvarlige at foretage underretning. Bestemmelsen skal således ses i sammenhæng med tilsynsmyndighedens beføjelser efter den foreslåede § 42.

Endeligt foreslås det i *§ 29, stk. 5*, at underretning af den registrerede kan udsættes, begrænses eller undlades af de grunde, der er nævnt i § 14, stk. 1.

Med den foreslåede bestemmelse sikres det, at en dataansvarlig kompetent myndighed ikke er forpligtet til at underrette en registreret om brud på datasikkerheden, hvis den registrerede ville have været afskåret fra at opnå indsigt efter den foreslåede § 15, jf. den foreslåede § 16, stk. 1.

Der henvises i øvrigt til pkt. 2.6.3.3 i lovforslagets almindelige bemærkninger.

Til § 30

Gældende ret indeholder ikke regler om databeskyttelsesrådgivere.

Den foreslås i *stk. 1*, at den dataansvarlige på grundlag af faglige kvalifikationer, herunder navnlig ekspertise inden for databeskyttelsesret og -praksis samt evnen til at udføre de opgaver, der er nævnt i kapitel 15, udpeger en databeskyttelsesrådgiver, som inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger.

Databeskyttelsesgiveren kan være en af den dataansvarliges eksisterende medarbejdere, som har fået særlig uddannelse inden for databeskyttelsesret og -praksis for at tilegne sig ekspertise på dette område. Vedkommendes opgaver vil kunne udføres på deltid eller fuldtid.

Databeskyttelsesrådgiveren vil endvidere kunne udpeges som databeskyttelsesrådgiver i forhold til databeskyttelsesforordningen.

Databeskyttelsesrådgiveren vil endvidere kunne fungere som kontaktpunkt, når der er tale om fælles dataansvarlige, jf. den foreslåede § 21.

Det foreslås videre i *stk. 2*, at flere dataansvarlige under hensyntagen til deres størrelse og organisatoriske forhold kan udpege en fælles databeskyttelsesrådgiver.

Med den foreslåede bestemmelse gives der mulighed for, at f.eks. politikredsene, som varetager både rollen som politi- og anklagemyndighed inden for den samme organisation, vil kunne udpege én databeskyttelsesrådgiver for al den behandling af personoplysninger, som foretages af politikredsen.

Det foreslås herudover i *stk. 3*, at forpligtelsen til at udpege en databeskyttelsesrådgiver ikke gælder for domstolene, når disse foretager behandling af personoplysninger inden for deres egenskab af domstole.

Med den foreslåede bestemmelse understreges det, at det særlige forhold ved domstolene, herunder navnlig domstolenes uafhængighed og den særlige ordning for tilsynet med domstolenes behandling af personoplysninger, indebærer, at der ikke skal udpeges en databeskyttelsesrådgiver for så vidt angår den behandling af personoplysninger, der foretages i forbindelse med domstolenes udøvelse af judicielle aktiviteter.

Endeligt foreslås det i *stk. 4*, at den dataansvarlige offentliggør kontaktoplysningerne for databeskyttelsesrådgiveren og meddeler disse til tilsynsmyndigheden.

Der henvises i øvrigt til pkt. 2.7.3 i lovforslagets almindelige bemærkninger.

Til § 31

Gældende ret indeholder ikke regler om databeskyttelsesrådgivere.

Det foreslås i § 31, at den dataansvarlige understøtter, at databeskyttelsesrådgiveren kan:

1) underrette og rådgive den dataansvarlige og de ansatte, der behandler personoplysninger, om deres forpligtelser i medfør af denne lov og anden lovgivning om databeskyttelse,
2) overvåge overholdelsen af denne lov og anden lovgivning om databeskyttelse og af den dataansvarliges politikker om beskyttelse af personoplysninger, herunder fordeling af ansvar, oplysningskampagner og uddannelse af det personale, der medvirker ved behandlingsaktiviteterne, og de tilhørende revisioner,
3) rådgive, når der anmodes herom, med hensyn til konsekvensanalysen vedrørende databeskyttelse og overvåge dens opfyldelse i henhold til bestemmelsen i § 25,
4) samarbejde med tilsynsmyndigheden, og
5) fungere som tilsynsmyndighedens kontaktpunkt i spørgsmål vedrørende behandling, herunder den forudgående høring, der er nævnt i § 26, og at høre tilsynsmyndigheden, når det er hensigtsmæssigt, om eventuelle andre spørgsmål.

Med den foreslåede bestemmelse slås det fast, hvilke opgaver databeskyttelsesrådgiveren skal løse.

Det vil være en naturlig del af databeskyttelsesrådgiverens opgaver, at der gives rådgivning også i forbindelse med udviklingen af nye automatiske databehandlingssystemer, da det vil være nærliggende, at databeskyttelsesrådgiveren har den fornødne viden om på den ene side den kompetente myndigheds behov for at foretage behandling af personoplysninger, og på den anden side de krav til overholdelse af behandlingsprincipper, sikkerhedskrav mv., som følger af den foreslåede lov.

Til § 32

Den foreslåede bestemmelse vedrører de generelle principper for overførsel til tredjelande.

Det foreslås i *§ 32, stk. 1,* at overførsel af personoplysninger, der behandles eller planlægges behandlet efter overførsel til et tredjeland eller en international organisation, herunder videreoverførsel til et andet tredjeland eller en anden international organisation, kun må finde sted under overholdelse af reglerne i lovforslaget, og hvis betingelserne i lovforslagets afsnit VII er overholdt, herunder navnlig at:

1) overførslen er nødvendig i forhold til de formål, der er nævnt i den foreslåede § 1, stk.1,
2) personoplysningerne overføres til en dataansvarlig i et tredjeland eller en international organisation, der er en myndighed, der er kompetent i forhold til de formål, der er nævnt i dem foreslåede § 1, stk.1,
3) hvor personoplysninger transmitteres eller stilles til rådighed af en kompetent myndighed fra en anden medlemsstat, denne myndighed har givet sin forudgående godkendelse til overførslen i henhold til dens nationale regler,
4) der foreligger et af de overførselsgrundlag, der er nævnt i kapitel 17, og
5) den kompetente myndighed, der foretog den oprindelige overførsel, i tilfælde af videreoverførsel til et andet tredjeland eller en anden international organisation, giver bemyndigelse til videreoverførslen, efter at den har taget behørigt hensyn til alle relevante faktorer, herunder den strafbare handlings grovhed, det formål, hvortil personoplysningerne oprindeligt blev overført, og beskyttelsesniveauet for personoplysninger i det tredjeland eller den internationale organisation, hvortil personoplysningerne videreoverføres.

Med den foreslåede bestemmelse fastlægges de generelle principper for, hvornår der kan ske overførsel til tredjelande eller internationale organisationer.

Det er således en betingelse, at overførsel er nødvendig af de formål, som fremgår af den foreslåede § 1 (*nr. 1*), at overførslen sker til myndigheder eller internationale organisationer, som er kompetente i forhold til disse

formål (*nr. 2*), og at der foreligger et af de overførselsgrundlag, som følger af de foreslåede §§ 33, 34 og 35 (*nr. 4*).

Et eksempel på en international organisation, der er kompetent i forhold til de formål, der fremgår af den foreslåede § 1, er Interpol.

Hvis der er tale om oplysninger, som er indsamlet i en anden medlemsstat, skal der endvidere foreligge en forudgående godkendelse fra den kompetente myndighed i den pågældende medlemsstat (*nr. 3*).

Hvis der er tale om en videreoverførsel fra et tredjeland eller international organisation til et andet tredjelande eller international organisation, skal der endvidere foreligge en tilladelse fra den kompetente myndighed, som foretog den oprindelig overførsel (*nr. 5*). Dette indebærer, at der ved en overførsel skal være en kontrol med den *efterfølgende* overførsel af oplysningerne.

Det foreslås dog videre i *§ 32, stk. 2*, at der skal kunne ske overførsel uden forudgående godkendelse efter stk. 1, nr. 3, hvis overførslen er nødvendig for at forebygge en umiddelbar og alvorlig trussel mod en medlemsstats eller et tredjelands offentlige sikkerhed eller mod en medlemsstats væsentlige interesser, og den forudgående godkendelse ikke kan indhentes i tide. Den myndighed, der er ansvarlig for at give den pågældende godkendelse, underrettes straks om overførslen.

Med den foreslåede bestemmelse sikres det, at der er mulighed for at overføre oplysninger uden at skulle afvente en godkendelse fra den kompetente myndighed i den medlemsstat, hvor oplysningerne er indsamlet, hvis der foreligger kvalificerede omstændigheder.

Til § 33

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

Spørgsmålet om, hvorvidt et tredjeland har et tilstrækkeligt beskyttelsesniveau, er i praksis knyttet til Europa-Kommissionens såkaldte tilstrækkelighedsafgørelser, som er bindende for medlemsstaterne. Foreligger der en sådan afgørelse, kan medlemsstaterne videregive oplysninger til det pågældende tredjeland på samme måde som til en anden medlemsstat.

Det foreslås i *§ 33*, at overførsel til tredjelande mv. kan ske, hvis Europa-Kommissionen har truffet afgørelse om, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation har et tilstrækkeligt beskyttelsesniveau.

Med den foreslåede bestemmelse gives der mulighed for, at der fremover kan ske overførsel af personoplysninger til tredjelande på baggrund af en tilstrækkelighedsafgørelse fra Europa-Kommissionen.

Kommissionens adgang til at træffe sådanne afgørelser følger af retshåndhævelsesdirektivets artikel 36. Som følge af, at retshåndhævelsesdirektivet finder anvendelse for de øvrige medlemsstater fra den 6. maj 2018, vil overførsler på baggrund af tilstrækkelighedsafgørelser fra Kommissionen først være relevant efter dette tidspunkt.

Der henvises i øvrigt til pkt. 2.8.3 i lovforslagets almindelige bemærkninger.

Til § 34

Det fremgår af persondatalovens § 27, stk. 1, at der udover overførsler på baggrund af et tilstrækkeligt beskyttelsesniveau kan ske overførsel, hvis en af de i stk. 3, nr. 1-8, nævnte betingelser er opfyldt.

Overførsel efter stk. 3 kan bl.a. ske, såfremt overførsel er nødvendig af hensyn til forebyggelse, efterforskning og forfølgning af strafbare forhold samt straffuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig forfølgning eller overførsel er nødvendig af hensyn til den offentlige sikkerhed, rigets forsvar eller statens sikkerhed.

Der kan endvidere ske overførsel, hvis den dataansvarlige i tredjelandet yder tilstrækkelige garantier for beskyttelse af den registreredes rettigheder, og tilsynsmyndigheden har givet særlig tilladelse hertil, eller på baggrund af kontrakter, der er i overensstemmelse med standardkontraktbestemmelser, som er godkendt af Europa-Kommissionen, jf. stk. 4 og 5.

Herudover skal persondatalovens almindelige behandlingsregler mv. være opfyldt ved overførsel af oplysninger til tredjelande efter stk. 1 og 3-5, jf. stk. 6.

Rammeafgørelsesbekendtgørelsens §§ 4-6 indeholder særlige regler om overførsel til tredjelande eller internationale organer af personoplysninger, som er modtaget fra eller stillet til rådighed af en anden medlemsstat.

Det fremgår af § 4, stk. 1, at videregivelse kun må ske, hvis det er nødvendigt for forebyggelse, efterforskning, afsløring eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner, og den modtagende myndighed i tredjelandet eller det modtagende internationale organ har ansvaret for at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner.

Det kræves endvidere, at den videregivende myndighed i den medlemsstat, som har sendt eller stillet oplysninger til rådighed, har givet sin godkendelse til at videregive disse i henhold til sin nationale lovgivning, og at det pågældende tredjeland eller internationale organ sikrer et tilstrækkeligt beskyttelsesniveau for den påtænkte behandling af oplysningerne.

Der kan dog efter stk. 2 ske videregivelse uden forhåndsgodkendelse fra den videregivende myndighed i den medlemsstat, som har sendt eller stillet oplysninger til rådighed, hvis videregivelsen af oplysningerne er afgørende for forebyggelse af en umiddelbar og alvorlig trussel mod den offentlige sikkerhed i et tredjeland eller et land inden for Den Europæiske Union eller Schengen-samarbejdet, eller videregivelsen af oplysningerne er afgørende for væsentlige interesser for et land inden for Den Europæiske Union eller Schengen-samarbejdet.

Det er en betingelse for videregivelsen, at forhåndsgodkendelse ikke kan indhentes i tide, og den udenlandske myndighed, der skulle have givet sin godkendelse, skal orienteres omgående.

Der kan efter bestemmelsens stk. 3 ske videregivelse i tilfælde, hvor det pågældende tredjeland eller internationale organ ikke sikrer et tilstrækkeligt beskyttelsesniveau for den påtænkte behandling af oplysningerne, hvis lovgivningen giver mulighed herfor på grund af den registreredes specifikke legitime interesser, eller på grund af legitime vigtige interesser, navnlig vigtige offentlige interesser, eller tredjelandet eller det modtagende internationale organ giver sikkerhedsgarantier, som den videregivende myndighed anser for tilstrækkelige i henhold til sin nationale lovgivning.

Det foreslås i *§ 34*, at hvis der ikke foreligger en tilstrækkelighedsafgørelse, jf. den foreslåede § 33, kan der ske overførsel, hvis:

1) der er givet de fornødne garantier, hvad angår beskyttelsen af personoplysninger, i en international aftale, eller
2) den dataansvarlige har vurderet alle forhold i forbindelse med overførslen af personoplysninger og konkluderer, at der findes de fornødne garantier for beskyttelsen af personoplysninger.

Med den foreslåede bestemmelse etableres et alternativ til overførsel på grundlag af en tilstrækkelighedsafgørelse fra Europa-Kommissionen. Der er tale om overførsler til kompetente myndigheder i tredjelande.

Formålet med de fornødne garantier er at sikre, at databeskyttelseskravene og de registreredes rettigheder opfyldes, herunder retten til effektiv administrativ eller retslig prøvelse.

Ved vurderingen af, om der foreligger de fornødne garantier, kan der inddrages eventuelle samarbejdsaftaler, der er indgået mellem Europol eller Eurojust og tredjelande, som tillader udveksling af personoplysninger. Det kan endvidere inddrages, om overførslen af personoplysninger vil være underlagt tavshedspligt og, at oplysningerne ikke bliver behandlet til andre formål end formålene med overførslen.

Det foreslås videre i *§ 34, stk. 2*, at den dataansvarlige skal underrette tilsynsmyndigheden om kategorier af overførsler i medfør af stk. 1, nr. 2, dvs. hvor overførsel sker, uden at der foreligger en international aftale herom.

Det foreslås endeligt i *§ 34, stk. 3*, at en overførsel i medfør af stk. 1, nr. 2, dokumenteres i forhold til dato og tidspunkt for overførslen, oplysninger om den modtagende kompetente myndighed, begrundelsen for overførslen og de overførte personoplysninger. Dokumentationen skal efter anmodning stilles til rådighed for tilsynsmyndigheden.

Der henvises i øvrigt til pkt. 2.8.3 i lovforslagets almindelige bemærkninger.

Til § 35

Det fremgår af persondatalovens § 27, stk. 1, at der udover overførsler på baggrund af et tilstrækkeligt beskyttelsesniveau kan ske overførsel, hvis en af de i stk. 3, nr. 1-8, nævnte betingelser er opfyldt.

Overførsel efter stk. 3 kan bl.a. ske, såfremt overførsel er nødvendig af hensyn til forebyggelse, efterforskning og forfølgning af strafbare forhold samt straffuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig forfølgning eller overførsel er nødvendig af hensyn til den offentlige sikkerhed, rigets forsvar eller statens sikkerhed.

Det foreslås i *§ 35*, at hvis der ikke foreligger afgørelse som nævnt i den foreslåede § 33 eller de fornødne garantier som nævnt i den foreslåede § 34, kan en overførsel eller en kategori af overførsler kun finde sted, hvis overførslen er nødvendig:

1) for at beskytte den registreredes eller en anden persons vitale interesser,
2) for at beskytte den registreredes legitime interesser, hvis det er fastsat i henhold til lov,
3) for at afværge en umiddelbar og alvorlig trussel mod en medlemsstats eller et tredjelands offentlige sikkerhed,
4) i enkeltsager med henblik på de formål, der er nævnt i § 1, stk. 1, eller
5) i en enkeltsag for, at retskrav kan fastlægges, gøres gældende eller forsvares med henblik på de formål, der er nævnt i § 1, stk. 1.

Med den foreslåede bestemmelsen etableres der et alternativt overførselsgrundlag, hvis der ikke foreligger en tilstrækkelighedsafgørelse eller de fornødne garantier. Overførsel kan således ske, hvis det er nødvendigt af hensyn til et af de nærmere angivne særlige formål. Overførsel i medfør af denne bestemmelse skal alene ske undtagelsesvist og skal begrænses til de oplysninger, som er strengt nødvendige for at varetage det pågældende formål.

De generelle principper i den foreslåede § 32 skal også overholdes ved en overførsel i medfør af den foreslåede § 35, idet en overførsel i medfør af *nr. 3* dog vil kunne ske uden forudgående godkendelse fra den indsamlende kompetente myndighed i en anden medlemsstat, jf. den foreslåede § 32, stk. 2.

Det foreslås således i *§ 35, stk. 2*, overførsel efter stk. 1, nr. 4 og 5, dvs. i enkeltsager, ikke kan finde sted, hvis hensynet til den registreredes rettigheder går forud for den samfundsmæssige interesse i overførslen. Hvis der f.eks. er tale om oplysninger vedrørende efterforskning af strafbare for-

hold, skal der tages hensyn til det strafbare forholds karakter, idet overførsel således ikke bør ske, hvis der er tale om mindre alvorlig kriminalitet.

Det foreslås endeligt i *§ 35, stk. 3,* en overførsel i medfør af stk. 1 dokumenteres i forhold til dato og tidspunkt for overførslen, oplysninger om den modtagende kompetente myndighed, begrundelsen for overførslen og de overførte personoplysninger. Dokumentationen skal efter anmodning stilles til rådighed for tilsynsmyndigheden.

Der henvises i øvrigt til pkt. 2.8.3 i lovforslagets almindelige bemærkninger.

Til § 36

Den foreslåede bestemmelse vedrører overførsel af oplysninger til modtagere, der ikke er kompetente i forhold til de formål, der er nævnt i dem foreslåede § 1, stk.1.

Det foreslås i *§ 36, stk. 1,* at de kompetente myndigheder kan overføre personoplysninger til andre end kompetente myndigheder og internationale organisationer på baggrund af international aftale eller i enkeltstående og specifikke tilfælde, hvis:

1) overførslen er strengt nødvendig for den overførende kompetente myndigheds udførelse af en af lovgivningen følgende opgave og forfølger de formål, der er nævnt i § 1, stk. 1,
2) den overførende kompetente myndighed fastslår, at ingen af den pågældende registreredes grundlæggende går forud for samfundets interesse, der nødvendiggør overførslen i det foreliggende tilfælde,
3) den overførende kompetente myndighed mener, at overførslen til en myndighed, der i tredjelandet er kompetent i forhold til de formål, der er nævnt i § 1, stk.1, er ineffektiv eller uhensigtsmæssig, navnlig fordi overførslen ikke kan foretages i tide,
4) den myndighed, der i tredjelandet er kompetent i forhold til de formål, der er nævnt i § 1, stk. 1, underrettes uden unødig forsinkelse, medmindre dette er ineffektivt eller uhensigtsmæssigt, og
5) den overførende kompetente myndighed underretter modtageren om det eller de specifikke formål, hvortil sidstnævnte udelukkende kan behandle personoplysningerne, forudsat at denne behandling er nødvendig.

Med den foreslåede bestemmelse gives der mulighed for, at der undtagelsesvist kan ske overførsel af oplysninger til andre end kompetente myndigheder og internationale organisationer.

Overførsel kan for det første ske på baggrund af en international aftale.

Overførsel kan for det andet ske i enkeltstående og specifikke tilfælde, hvis en række nærmere angivne betingelser er opfyldt. Overførsel efter bestemmelsen kan ske, hvis en overførsel til en kompetent myndighed i det pågældende tredjeland vil være ineffektive eller uhensigtsmæssige, navnlig fordi overførslen ikke kunne gennemføres rettidigt, eller fordi den nævnte myndighed i tredjelandet ikke respekterer retsstatsprincippet eller internationale menneskerettighedsnormer og –standarder.

Overførsel efter bestemmelsen kan være relevant, hvis der er akut behov for at overføre personoplysninger for at redde en persons liv, som er i fare for at blive offer for en strafbar handling, eller for at forhindre en nært forestående forbrydelse, herunder terrorisme.

Det foreslås videre i *§ 36, stk. 2*, at den overførende kompetente myndighed skal dokumentere og underrette tilsynsmyndigheden om overførsler til modtagere, der ikke er kompetente myndigheder.

Der henvises i øvrigt til pkt. 2.8.3 i lovforslagets almindelige bemærkninger.

Til § 37

Til stk. 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.

Det foreslås i *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 19 om tilsyn med domstolene.

Med den foreslåede bestemmelse får tilsynet til opgave at føre tilsyn med behandling, der er omfattet af loven. Datatilsynet varetager således både tilsynet i forhold til persondataloven og – efter den 25. maj 2018 – databeskyttelsesforordningen samt den foreslåede lov.

Der henvises i øvrigt til pkt. 2.9.3 i lovforslagets almindelige bemærkninger.

Til stk. 2

Det fremgår af persondatalovens § 55, stk. 2, at Datatilsynets daglige forretninger varetages af sekretariatet, der ledes af en direktør.

Det foreslås i *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.

Til stk. 3

Det fremgår af persondatalovens § 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, s. 4101), at der ved udpegning af medlemmer af rådet skal tilstræbes uvildighed og sagkundskab.

Det foreslås i *stk. 3*, at justitsministeren nedsætter Datarådet, som består af en formand, der er dommer, og af 6 andre medlemmer. Der kan udpeges 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, herunder navnlig ekspertise inden for databeskyttelsesret.

Der sker med den foreslåede bestemmelse en videreførelse af reglerne om Datarådets nedsættelse med den ændring, at der alene kan ske genudpegning to gange.

Til stk. 4

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 *stk. 4*, at bemyndigelsen til, at Datarådet kan fastsætte sin forretningsorden og fordelingen af arbejdet mellem rådet og sekretariatet videreføres. Det bemærkes, at indtil rådet har fastsat en forretningsorden mv. i medfør af denne bestemmelse, vil den gældende forretningsorden fortsat gælde for Datarådets tilsyn i medfør af nærværende lov, jf. herved den foreslåede § 54, nr. 1 (den foreslåede § 2 a, stk. 2).

Til stk. 5

Det foreslås i *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 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).

Med den foreslåede bestemmelse sikres det, at Datarådet kan håndtere oplysninger om de kompetente myndigheders systemer på betryggende vis. Hvis et medlem mister sin sikkerhedsgodkendelse, vil den pågældende ikke længere kunne være medlem af rådet.

Til stk. 6 og 7

Det foreslås i *§ 37, stk. 6*, at hvervet som formand, medlem eller stedfortræder ophører ved udgangen af embedsperioden eller ved frivillig fratræden.

Det foreslås videre i *§ 37, 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 Rådet.

Der henvises i øvrigt til pkt. 2.9.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 8

Det fremgår af persondatalovens § 56, at Datatilsynet varetager sine opgaver i fuld uafhængighed.

Det fremgår af forarbejderne til persondataloven (Folketingstidende 1999-2000, tillæg A, s. 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 *stk. 8, at* sekretariatets personale samt Datarådets formand, medlemmer og stedfortrædere for disse kun kan have bibeskæftigelse, for så vidt og i det omfang det er foreneligt med udøvelsen af de til stillingen eller hvervet knyttede pligter.

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 pkt. 2.9.3.1 i lovforslagets almindelige bemærkninger.

Til stk. 9

Det foreslås i *§ 37, 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 varetage også Domstolsstyrelsens synspunkter som tilsynsmyndighed, jf. også den foreslåede § 46 om samarbejde mellem tilsynsmyndighederne.

Til § 38

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 videre 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 *stk. 1*, at Domstolsstyrelsen fører tilsyn med behandling af oplysninger, der foretages for domstolene, når disse handler uden for deres egenskab af domstol.

Det foreslås videre 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 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.

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 pkt. 2.9.3.2 i lovforslagets almindelige bemærkninger.

Til § 39

Det fremgår af persondatalovens § 56, at Datatilsynet udøver sine funktioner i fuld uafhængighed. Tilsvarende gælder for Domstolsstyrelsen, jf. § 68, stk. 1.

Det foreslås i *§ 38*, at det fastslås, at tilsynsmyndighederne udøver sine funktioner i fuld uafhængighed.

Der er således tale om videreførelse af gældende ret.

Der henvises i øvrigt til pkt. 2.9.3.3 i lovforslagets almindelige bemærkninger.

Til § 40

Til stk. 1

Det foreslås i *stk. 1*, at det fastlægges, at tilsynsmyndighederne har til opgave her i landet at:

1) føre tilsyn med og håndhæve anvendelsen af denne lov,
2) fremme offentlighedens kendskab til og forståelse af risici, regler, garantier og rettigheder i forbindelse med behandling af personoplysninger,
3) rådgive Folketinget, regeringen og andre institutioner og organer om lovgivningsmæssige og administrative foranstaltninger til beskyttelse af fysiske personers rettigheder i forbindelse med behandling,
4) fremme dataansvarliges og databehandleres kendskab til deres forpligtelser i medfør af denne lov,
5) efter anmodning informere alle registrerede om udøvelsen af deres rettigheder i medfør af denne lov og med henblik herpå samarbejde med tilsynsmyndighederne i andre medlemsstater, hvis det er relevant,
6) behandle klager, der indgives af en registreret eller af et organ, en organisation eller en sammenslutning i overensstemmelse med bestemmelsen i § 48, og, for så vidt det er hensigtsmæssigt, undersøge genstanden for klagen og underrette klageren om forløbet og resultatet af undersøgelsen inden for senest 3 måneder, navnlig hvis yderligere undersøgelse eller koordinering med en anden tilsynsmyndighed er nødvendig,
7) efter anmodning yde supplerende bistand til en registreret, der har indgivet en klage,

8) underrette en registreret, der har indgivet en klage, om adgangen til retsmidler efter kapitel 22,
9) efter anmodning kontrollere, om en behandling af personoplysninger er lovlig i henhold til udsættelse, begræsning, undladelse eller nægtelse efter kapitel 4-6, og underrette den registrerede inden for en rimelig frist om resultatet af undersøgelsen eller om årsagerne til, at undersøgelsen ikke er foretaget, og om den registreredes adgang til retsmidler efter kapitel 22,
10) samarbejde med andre tilsynsmyndigheder, herunder gennem udveksling af oplysninger og gensidig bistand med henblik på at sikre ensartet anvendelse og håndhævelse af denne lov,
11) gennemføre undersøgelser om anvendelsen af denne lov, herunder på grundlag af oplysninger, der er modtaget fra en anden tilsynsmyndighed eller en anden offentlig myndighed,
12) holde øje med relevant udvikling, for så vidt den har indvirkning på beskyttelse af personoplysninger, navnlig udviklingen for informations- og kommunikationsteknologi,
13) rådgive om behandlingsaktiviteter som omhandlet i § 26, og
14) bidrage til Databeskyttelsesrådets aktiviteter.

Med den foreslåede bestemmelse sker der en samlet oplistning af tilsynsmyndighedernes opgaver efter loven. Der er i vidt omfang tale om en videreførelse af gældende ret i forhold til de opgaver, som tilsynsmyndighederne varetager i dag.

Til stk. 2

Det foreslås i *stk. 2*, at tilsynsmyndighederne fastsætter nærmere regler for at lette indgivelsen af klager efter stk. 1, nr. 6.

Til stk. 3

Det foreslås i *stk. 3*, at tilsynsmyndighederne kan afvise at imødekomme åbenbart grundløse eller overdrevent gentagne anmodninger efter den foreslåede lov.

Det er tilsynsmyndigheden, som har bevisbyrden for, at betingelserne for, at der kan ske afvisning, er opfyldt. Det er således ikke op til den registrerede at godtgøre en berettiget interesse, men i det omfang, at den registrerede fremkommer med oplysninger om en sådan interesse, vil der formod-

ningsvist ikke være grundlag for at afvise anmodningen i medfør af den foreslåede bestemmelse.

Til § 41

Det fremgår af persondatalovens § 62, stk. 1, at Datatilsynet kan kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

Tilsynets medlemmer og personale har 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. § 62, stk. 2.

Tilsvarende gælder for Domstolsstyrelsen, jf. § 68, stk. 1.

Det foreslås i *stk.1*, at tilsynsmyndighederne kan kræve enhver oplysning, der er af betydning for deres virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

Det foreslås videre i s*tk. 2*, at tilsynsmyndighedernes medlemmer og personale til enhver tid mod behørig legitimation uden retskendelse har adgang til alle lokaler, hvorfra en behandling foretages.

Med den foreslåede bestemmelse sker der en videreførelse af gældende ret i forhold til spørgsmålet om tilsynsmyndighedernes adgang til oplysninger og til lokaler, hvorfra der foretages behandling af personoplysninger.

Til § 42

Til stk. 1

Det fremgår af persondatalovens § 59, at Datatilsynet kan påbyde en privat dataansvarlig at ophøre med en behandling, der ikke må finde sted efter denne lov, og at berigtige, slette eller blokere bestemte oplysninger, som er omfattet af en sådan behandling.

Tilsynet kan forbyde en privat dataansvarlig at anvende en nærmere angiven fremgangsmåde i forbindelse med behandlingen af oplysninger, hvis tilsynet finder, at den pågældende fremgangsmåde medfører en væsentlig risiko for, at der behandles oplysninger i strid med loven, jf. stk. 2.

Tilsynet kan i særlige tilfælde meddele databehandlere påbud eller forbud, jf. § 59, stk. 4.

Der er således efter gældende ret ikke mulighed for, at tilsynsmyndighederne kan meddele påbud eller forbud til offentlige myndigheder.

Det foreslås i *stk. 1*, at tilsynsmyndighederne over for den dataansvarlige og databehandleren kan afgive udtalelse om, at planlagte behandlingsaktiviteter sandsynligvis vil være i strid med nærværende lov, give påbud om at bringe behandlingsaktiviteter i overensstemmelse med nærværende lov, eller midlertidigt eller definitivt begrænse, herunder forbyde, behandling af personoplysninger.

Med den foreslåede bestemmelse sker der således en udvidelse af tilsynsmyndighedernes beføjelser over for de kompetente myndigheder i forhold til i dag.

Hvis den kompetente myndighed iværksætter behandlingsaktiviteter uden hensyntagen til en udtalelse fra tilsynsmyndigheden om, at behandlingsaktiviteten sandsynligvis ville være i strid med loven, , vil tilsynsmyndigheden kunne meddele påbud eller forbud i forhold til den pågældende behandlingsaktivitet.

En overtrædelse af et påbud eller forbud vil efter omstændighederne indebære, at den kompetente myndighed ifalder strafansvar, jf. herved den foreslåede § 50, stk. 2, og bemærkningerne hertil.

Til stk. 2

Det fremgår af persondatalovens § 61, at Datatilsynets afgørelser efter persondataloven ikke kan indbringes for anden administrativ myndighed. Tilsvarende gælder for Domstolsstyrelsen, jf. § 68, stk. 1, 2. pkt.

Det foreslås i *stk. 2*, at tilsynsmyndighedernes afgørelser efter den foreslåede lov ikke kan indbringes for anden administrativ myndighed.

Med den foreslåede bestemmelse sker der en videreførelse af gældende ret i forhold til spørgsmålet om adgangen til at indbringe tilsynsmyndighedernes afgørelser for anden administrativ myndighed.

Til § 43

Det fremgår af persondatalovens § 57, at ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger, skal der indhentes en udtalelse fra Datatilsynet. Tilsvarende gælder for Domstolsstyrelsen i forhold til behandling af personoplysninger ved domstolene, jf. § 68, stk. 2.

Det foreslås i *§* 43, at der ved udarbejdelse af generelle retsforskrifter, der har betydning for behandling af personoplysninger, skal der indhentes en udtalelse fra Datatilsynet. Hvis der er tale om generelle forskrifter, der har betydning for behandling af oplysninger, der foretages for domstolene, skal der indhentes en udtalelse fra Domstolsstyrelsen.

Med den foreslåede bestemmelse sker der således en videreførelse af gældende ret i forhold til forpligtelsen til at inddrage tilsynsmyndighederne.

Til § 44

Der er ikke efter gældende ret mulighed for, at tilsynsmyndighederne kan indbringe spørgsmål om overtrædelse af persondataloven for domstolene. Tilsynsmyndighederne kan anmelde forhold til politiet, hvorefter spørgsmålet om overtrædelse af loven behandles i en straffesag.

Det foreslås i *§ 44*, 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.

Til § 45

Det fremgår af persondatalovens § 65, at Datatilsynet afgiver en årlig beretning om sin virksomhed til Folketinget. Beretningen offentliggøres.

Domstolsstyrelsen offentliggør en årlig beretning om dens virksomhed, jf. § 68, stk. 3.

Det foreslås i *§ 45*, at tilsynsmyndighederne afgiver en årlig beretning om deres virksomhed til Folketinget og justitsministeren. Beretningerne offentliggøres.

Med den foreslåede bestemmelse sker der således i vidt omfang en videreførelse af gældende ret i forhold til tilsynsmyndighedernes pligt til at afgive en årsberetning.

Til § 46

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

Det foreslås i *§ 46*, at tilsynsmyndighederne samarbejder, i det omfang det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle relevante oplysninger.

Med den foreslåede bestemmelse sker der således en videreførelse af gældende ret i forhold til tilsynsmyndighedernes pligt til at samarbejde.

Til § 47

Persondataloven indeholder ikke regler om tilsynsmyndighedernes samarbejde med tilsynsmyndigheder fra andre medlemsstater.

Det foreslås i *stk. 1*, at tilsynsmyndighederne uden unødig forsinkelse og senest en måned efter modtagelsen besvarer en anmodning fra en tilsynsmyndighed i en anden medlemsstat. Oplysninger, som en tilsynsmyndighed i en anden tilsynsmyndighed har anmodet om, fremsendes elektronisk i et standardformat.

Det foreslås videre i *stk. 2*, at anmodninger om bistand skal indeholde alle nødvendige oplysninger, herunder formålet med og grunden til anmodningen. Udvekslede oplysninger må kun anvendes til det formål, som er angivet i anmodningen.

Endeligt foreslås det i *stk. 3*, at anmodninger alene kan afvises, når den anmodede tilsynsmyndighed ikke har kompetence med hensyn til genstanden for anmodningen eller de foranstaltninger, som den anmodes om at iværksætte, eller en imødekommelse af anmodningen vil være i strid med denne eller anden lov. Et afslag på at imødekomme en anmodning skal begrundes.

Tilsynsmyndigheden vil således ikke kunne imødekomme en anmodning om, at der meddeles et påbud om at forbyde en behandling, som ikke er omfattet af den foreslåede lovs anvendelsesområde, eller hvis den pågældende behandling overholder reglerne i den foreslåede lov.

Til § 48

Til stk. 1

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.

Til stk. 2

Det foreslås i *stk. 2*, at tilsynsmyndighedernes afgørelser, undladelser af at behandle en klage fra en registreret eller en manglende underretning efter § 38, stk. 1, nr. 6, af den registrerede eller dennes repræsentant kan indbringes for domstolene efter retsplejelovens regler.

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, 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 den foreslåede § 38, stk. 1, nr. 6. 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.

Til stk. 3

Det foreslås i stk. 3, at den registrerede eller den registreredes repræsentant kan indbringe spørgsmål om dataansvarliges og databehandleres 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, at den registrerede kan indbringe overensstemmelse 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 pkt. 2.10.3.2-2.10.3.4 i lovforslagets almindelige bemærkninger.

Til § 49

Det fremgår af persondatalovens § 69, at den dataansvarlige skal 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.

Af den gældende erstatningsregel i persondatalovens § 69 følger der således et skærpet ansvarsgrundlag i form af et præsumptionsansvar (culpa med omvendt bevisbyrde) for den dataansvarlige. Herudover finder de almindelige erstatningsretlige principper anvendelse.

Det foreslås i *§ 49*, at enhver person, som har lidt materiel eller immateriel skade som følge af en ulovlig behandlingsaktivitet eller enhver anden behandling i strid med denne lov, har ret til erstatning fra den dataansvarlige i overensstemmelse med de almindelige erstatningsretlige principper.

Bestemmelsen indebærer således, at en person, som har lidt et tab som følge af en ansvarspådragende handling i form af ulovlig behandling af personoplysninger, har ret til erstatning. Bestemmelsen indebærer endvidere, at retten til erstatning følger af dansk rets almindelige erstatningsretlige principper. Det betyder, at det er en betingelse for at ifalde et erstatningsansvar, at der er sket en skade, hvormed der er lidt et økonomisk tab, og at skadevolderen kan gøres ansvarlig for skaden efter den almindelige culpanorm, dvs. at skadevolderen har handlet culpøst og forvoldt skaden ved forsætlig eller uagtsom adfærd.

Det er endvidere en betingelse for, at skadevolderen kan ifalde et erstatningsansvar, at der foreligger den nødvendige årsagsforbindelse (kausalitet) mellem den indtrådte skade og skadevolderens adfærd. Herved forstås, at den skadevoldende adfærd har forøget risikoen for, at den pågældende skade indtræder. Herudover forudsætter et erstatningsansvar, at der foreligger såkaldt adækvans (påregnelighed), dvs. at skaden er en påregnelig følge af skadevoldernes adfærd. Skader, der er helt atypiske eller tilfældige i forhold til den risiko, som skadevolders adfærd har fremkaldt, falder dermed normalt uden for erstatningspligten.

Der henvises i øvrigt til pkt. 2.10.3.5 i lovforslagets almindelige bemærkninger.

Til § 50

Til stk. 1 og 2

Det fremgår af persondatalovens § 70, stk. 2, at 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 tredjemand i statistisk eller videnskabeligt øjemed), § 13, stk. 1 (om registrering af udgående telefonopkald), § 27, stk. 4 (overførsel af oplysninger til tredjelande), eller en betingelse eller et vilkår for en tilladelse i henhold til regler udstedt i medfør af loven.

Strafansvar efter § 70, stk. 2, vedrører primært bestemmelser, som private databehandlere, der udfører opgaver for offentlige myndigheder, skal iagttage.

Strafansvar i forhold til den offentlige myndighed er navnlig relevant ved overtrædelser af vilkår fastsat af Datatilsynet. Strafansvaret suppleres i disse situationer af straffelovens regler samt af adgangen for myndigheden til at iværksætte disciplinære sanktioner over for den fysiske person, dvs. den ansatte, som har overtrådt persondataloven.

Det foreslås i *stk. 1*, at medmindre højere straf er forskyldt efter anden lovgivning, kan en privat databehandler, der i forbindelse med en behandling, der udføres for en kompetent myndighed, overtræder § 22, stk. 2 og 3, § 23, stk. 2, § 27 og § 28, stk. 2, eller undlader at efterkomme et påbud eller forbud, der er meddelt i henhold til § 42, straffes med bøde eller fængsel indtil 4 måneder.

Med den forslåede bestemmelse kan der således idømmes straf i form af bøde eller fængsel, hvis en privat databehandler overtræder den foreslåede § 22 om kravene til databehandlere, herunder kravene til gennemførsel af en behandling ved en databehandler og anvendelse af underdatabehandlere. Endvidere strafbelægges databehandleren pligt til at føre skriftlige fortegnelser over alle kategorier af behandlingsaktiviteter efter § 23, stk. 2, samt bestemmelsen i § 27 om behandlingssikkerhed. Endelig strafbelægges databehandlerens pligt til at underrette den dataansvarlige om brud på persondatasikkerheden efter § 28, stk. 2, samt en databehandlers manglen-

de efterkommelse af et påbud eller forbud, der er meddelt af en tilsynsmyndighed i henhold til lovens § 42.

Der er således til dels tale om en videreførelse af den gældende bestemmelse i persondatalovens § 70, stk. 2, hvorefter en privat databehandler kan straffes for overtrædelse af persondatalovens § 41, stk. 3.

Det foreslås i s*tk. 2*, at medmindre højere straf er forskyldt efter anden lovgivning, kan dataansvarlige, der undlader at efterkomme et påbud eller forbud, der er meddelt i henhold til § 42, straffes med bøde.

Med den foreslåede bestemmelse fastslås det, at offentlige myndigheder kan ifalde strafansvar i form af bøde, hvis myndigheden undlader at efterkomme et påbud eller forbud, som tilsynsmyndigheden har meddelt i henhold til den foreslåede § 42.

Det sikres herved, at sanktioneringen af de kompetente myndigheders overtrædelser af nærværende lov i første omgang håndteres af tilsynsmyndigheden gennem meddelelse af påbud eller forbud. Overtrædes et sådant påbud eller forbud, vil tilsynsmyndigheden kunne anmelde forholdet til politiet, som vurderer, om der er grundlag for at rejse en straffesag.

Strafansvaret over for myndigheden vil på samme måde som i dag være suppleret af straffelovens regler samt af adgangen for myndigheden til at iværksætte disciplinære sanktioner over for ansatte, som foretager behandling i strid med loven.

Der henvises i øvrigt til pkt. 2.10.3.6 i lovforslagets almindelige bemærkninger.

Til stk. 3 og 4

Det fremgår af persondatalovens § 70, stk. 4, at i regler, der udstedes i medfør af loven, kan der fastsættes straf af bøde eller hæfte.

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

Det foreslås i *stk. 3*, at i regler, der udstedes i medfør af loven, kan der fastsættes straf af bøde eller fængsel indtil 4 måneder.

Der sker med den foreslåede bestemmelse en videreførelse af adgangen til at fastsatte strafbestemmelser i regler, der udstedes i medfør af loven, idet adgangen hertil dog – i overensstemmelse med den foreslåede § 50, stk. 1 og 2 – begrænses til fængsel i op til 4 måneder.

Det foreslås videre i *stk. 4*, at der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Der sker med den foreslåede bestemmelse en videreførelse af gældende ret. Efter straffelovens § 27, stk. 2, kan statslige myndigheder og kommuner alene straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private.

Der henvises i øvrigt til pkt. 2.10.3.6 i lovforslagets almindelige bemærkninger.

Til § 51

Det fremgår af persondatalovens § 75, at justitsministeren kan fastsætte regler, som er nødvendige for at gennemføre de af Det Europæiske Fællesskab udstedte beslutninger, som træffes med henblik på gennemførelse af direktivet om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, eller regler, som er nødvendige for at anvende de af Fællesskabet udstedte retsakter på direktivets område.

Det foreslås i *§ 51*, at justitsministeren bemyndiges til at fastsætte regler, som er nødvendige for at gennemføre de af Europa-Kommissionen udstedte retsakter, som træffes med henblik på gennemførelse af direktivet 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, eller regler, som er nødvendige for at anvende de af Europa-Kommissionen udstedte retsakter på direktivets område.

Med den foreslåede bestemmelse tilvejebringes det fornødne grundlag for justitsministeren til om nødvendigt at fastsætte administrative bestemmelser til opfyldelse af de gennemførelsesretsakter, som Europa-

Kommissionen måtte vedtage efter proceduren i retshåndhævelsesdirektivets artikel 58, jf. artikel 36 om tilstrækkelighedsafgørelser og artikel 50 om procedurer for gensidig bistand mellem tilsynsmyndighederne.

Til § 52

Det foreslås i *stk. 1*, at loven træder i kraft dagen efter bekendtgørelse i Lovtidende.

Det foreslås i *stk. 2*, at lovforslaget kan stadfæstes straks efter dets vedtagelse.

Bestemmelsen skal ses i lyset af, at gennemførslen af retshåndhævelsesdirektivet skal ske inden den 1. maj 2017, idet gennemførslen er en forudsætning for, at der kan indgås en samarbejdsaftale mellem Danmark og Europol, som skal have virkning fra samme dato.

Der er således behov for hurtigst muligt at træffe de foranstaltninger, der er nødvendige for, at direktivet kan gennemføres i Danmark.

Der henvises i øvrigt til pkt. 1.1 i lovforslagets almindelige bemærkninger.

Til § 53

Det foreslås i stk. 1, at lovens § 25 og § 26 gælder i forhold til behandling af personoplysninger, der foretages, og registre, der oprettes, den 1. maj 2017 eller senere.

Med den foreslåede bestemmelse understreges det, at de foreslåede bestemmelser om henholdsvis konsekvensanalyser og forudgående høring af tilsynsmyndigheden finder anvendelse i forhold til ny behandling, der iværksættes, og registre, der oprettes, på tidspunktet for lovens ikrafttræden eller senere.

Det foreslås videre i *stk. 2*, at lovens § 20, stk. 2, gælder i forhold til automatiske databehandlingssystemer, der idriftsættes den 1. maj 2017 eller senere.

Med den foreslåede bestemmelse understreges det, at den foreslåede bestemmelse om databeskyttelse gennem design og gennem standardindstil-

linger finder anvendelse i forhold til automatiske databehandlingssystemer, der sættes i drift på tidspunktet for lovens ikrafttræden eller senere.

Til § 54

Det foreslås i *§ 54*, at overførsler til tredjelande og internationale organisationer kan ske i medfør af internationale aftaler, der er indgået inden den 6. maj 2016, indtil de ændres, erstattes eller ophæves.

Det sikres herved, at der fortsat kan ske overførsler af personoplysninger til tredjelande og internationale organisationer i medfør af internationale aftaler, som overholdt de regler om databeskyttelse, der gjaldt inden den 6. maj 2016, hvor retshåndhævelsesdirektivet trådte i kraft. Der kan f.eks. være tale om aftaler om overførsel af personoplysninger til den internationale politiorganisation Interpol.

Til § 55

Den foreslåede bestemmelse vedrører konsekvensændringer i persondataloven.

Det foreslås i *nr. 1*, at persondatalovens § 2, stk. 4, ophæves.

Med den foreslåede bestemmelse ophæves persondatalovens bestemmelse om lovens anvendelsesområde i forhold til politiet, anklagemyndigheden og domstolene på det strafferetlige område. Bestemmelsen skal således ses i sammenhæng med den foreslåede ændring i nr. 2.

Det foreslås i *nr. 2*, at der indsættes en ny § 2 a, stk. 1, i persondataloven, hvorefter persondataloven ikke gælder for behandling, som er omfattet af den foreslåede lov om retshåndhævende myndigheders behandling af personoplysninger.

Det foreslås endvidere, at der indsættes en ny § 2 a, stk. 2, hvorefter de regler, som er udstedt i medfør af persondatalovens § 32, stk. 5, § 41, stk. 5, § 55, stk. 4, § 72 og § 72 a fortsat gælder for den behandling af personoplysninger, der er omfattet af lov om retshåndhævende myndigheders behandling af personoplysninger. Reglerne gælder ikke, hvis det vil være i strid med denne lov.

Med den foreslåede bestemmelse fastslås det, at persondataloven ikke længere for anvendelse i forhold til den behandling af personoplysninger, der er omfattet af den foreslåede lov.

Der er imidlertid udstedt en række bekendtgørelser med hjemmel i persondataloven, som har betydning for de kompetente myndigheders behandling af personoplysninger inden for den foreslåede lovs anvendelsesområde.

Med den foreslåede bestemmelse sikres det, at disse bekendtgørelser fortsat finder anvendelse for de kompetente myndigheders behandling af personoplysninger. De pågældende bekendtgørelser kan erstattes af nye regler, som udstedes i medfør af den foreslåede lov.

Der er tale om bekendtgørelse om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG), bekendtgørelse om behandling af personoplysninger, der leveres eller modtages i henhold til Prümafgørelsen om udveksling af oplysninger om dna-profiler, fingeraftryk og køretøjer m.v., bekendtgørelse om behandling af personoplysninger i Det Centrale Kriminalregister (Kriminalregisteret), bekendtgørelse om behandling af personoplysninger i Politiets Efterforskningsstøtte Database (PED), bekendtgørelse om forretningsorden for Datarådet, sikkerhedsbekendtgørelsen for domstolene og sikkerhedsbekendtgørelsen.

Anvendelsen af bekendtgørelserne skal ske i lyset af den foreslåede § 2 og bemærkningerne hertil. Bekendtgørelsernes regler finder således anvendelse i det omfang, at disse ikke strider mod reglerne i retshåndhævelsesdirektivet.

Til § 56

Bestemmelsen vedrører lovens territoriale gyldighed.

Det fremgår af persondatalovens § 83, at loven ikke gælder for Færøerne, men at loven ved kongelig anordning kan sættes i kraft for rigsmyndighedernes behandling af oplysninger med de afvigelser, som de særlige færøske forhold tilsiger. Loven gælder heller ikke for Grønland, men kan ved kongelig anordning sættes i kraft med de afvigelser, som de særlige grønlandske forhold tilsiger.

Persondataloven er ved anordning nr. 1238 af 14. oktober 2016 sat kraft for Grønland.

Det foreslås i *§ 55*, at loven ikke skal gælde for Færøerne, men at loven ved kongelig anordning kan sættes i kraft for rigsmyndighedernes behandling af oplysninger med de afvigelser, som de færøske forhold tilsiger. Loven gælder heller ikke for Grønland, men kan ved kongelig anordning sættes i kraft med de afvigelser, som de grønlandske forhold tilsiger.