



JUSTITSMINISTERIET

Lovafdelingen

Dato:
Kontor: Databeskyttelseskontoret
Sagsbeh: Kenny Rasmussen
Sagsnr.: 2016-7910-0008
Dok.: 2258100

KOMMENTERET OVERSIGT

over

høringssvar om forslag til lov om retshåndhævende myndigheders behandling af personoplysninger (Gennemførelse af direktiv om data- beskyttelse på retshåndhævelsesområdet)

1. Høringen

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

Østre Landsret, Vestre Landsret, byretterne, Datatilsynet, Direktoratet for Kriminalforsorgen, Dommerfuldmægtigforeningen, Domstolsstyrelsen, Rigsadvokaten, Rigspolitiet, Skatteministeriet, Advokatrådet, Landsforeningen af Forsvarsadvokater, Danske Advokater, Den Danske Dommerforening, Foreningen af Offentlige Anklagere, Institut for Menneskerettigheder, Politiforbundet, Foreningen af fængselsinspektører, vicefængselsinspektører og økonomichefer, Fængselsforbundet i Danmark, HK Landsklubben Kriminalforsorgen, Kriminalforsorgsforeningen og Landsklubben af socialrådgivere ansat i Kriminalforsorgen.

Udkast til lovforslag har endvidere været sendt i høring hos Færøernes Landsstyre og Grønlands Selvstyre.

Justitsministeriet har modtaget høringssvar fra:

Advokatrådet, Datatilsynet, Den Uafhængige Politiklagemyndighed, Direktoratet for Kriminalforsorgen, Domstolsstyrelsen, Institut for Menneskerettigheder, IT-Politisk Forening, Københavns Byret, Skatteministeriet,

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Sø- og Handelsretten, Rigsadvokaten, Rigspolitiet, Vestre Landsret og Østre Landsret.

Nedenfor er gengivet de væsentligste punkter i de modtagne høringssvar. Justitsministeriets kommentarer til høringssvarene er anført i *kursiv*.

2. Høringssvarene

2.1. Generelt

Advokatrådet, Direktoratet for Kriminalforsorgen, Københavns Byret, Sø- og Handelsretten, Skatteministeriet, Vestre Landsret og Østre Landsret har ikke haft bemærkninger til lovudkastet.

Datatilsynet anbefaler, at der indsættes en definition af begrebet ”pseudonymisering”, idet tilsynet peger på, at det er en udbredt misforståelse, at ”pseudonymisering” er sammenfaldende med ”anonymisering”, hvilket kan betyde, at der foretages en ulovlig behandling af personoplysninger.

Den Uafhængige Politiklagemyndighed bemærker, at lovforslaget bør indeholde en kort beskrivelse af retsplejelovens kapitel 93 c om straffesager mod politipersonale.

IT-Politisk Forening bemærker, at lovforslagets § 55, stk. 2, indebærer, at regler udstedt i medfør af persondataloven fortsat finder anvendelse, medmindre det vil være i strid med lovforslagets regler. IT-Politisk Forening finder, at det skaber en usikkerhed om retstilstanden, og at det ikke kan overlades til borgerne at vurdere, om en given regel i en bekendtgørelse, som er udstedt i medfør af persondataloven, ikke længere finder anvendelse, fordi den er i strid med lovforslaget og retshåndhævelsesdirektivet. Justitsministeriet bør derfor hurtigst muligt revidere de eksisterende bekendtgørelser. IT-Politisk Forening peger endvidere på, at begrebet ”lov” generelt skal fortolkes i lyset af praksis fra EU-Domstolen og Den Europæiske Menneskerettighedsdomstol, hvorefter der er krav om, at et retsgrundlag skal være tilstrækkeligt klart og præcist, og at anvendelsen heraf skal være forudsigelig for de personer, der er omfattet af retsgrundlagets anvendelsesområde.

Rigspolitiet noterer sig, at der i lovforslaget er hjemmel til at udstede administrative regler for bl.a. oplysningspligten, indsigtsretten og behandlingssikkerheden. Fastsættelsen af nærmere regler for disse områder vil i

praksis have væsentlig betydning for dansk politis implementering og efterlevelse af de nye regler.

For så vidt angår behovet for, at der indsættes en definition af begrebet "pseudonymisering", bemærker Justitsministeriet, at begrebet "pseudonymisering" ikke anvendes i lovforslagets lovtekst. Justitsministeriet finder på den baggrund, at det ikke er hensigtsmæssigt, at definitionen af begrebet indgår i lovteksten. Rets håndhævelsesdirektivets definition på begrebet er imidlertid beskrevet i de specielle bemærkninger til lovforslagets § 20, idet pseudonymisering indgår som et eksempel på databeskyttelse gennem design. Justitsministeriet har herved også lagt vægt på, at lovforslaget retter sig mod offentlige myndigheder, som må forventes at være bekendt med forskellen på anonymisering og pseudonymisering.

Justitsministeriet er enig med Den Uafhængige Politiklagemyndighed i, at lovforslagets bemærkninger bør indeholde en kort beskrivelse af retsplejelovens kapitel 93 c.

Justitsministeriet er endvidere enig med IT-Politisk Forening og Rigspolitiet i, at hensynet til på den ene side de registreredes rettigheder og på den anden side de kompetente myndigheders implementering og efterlevelse af de nye regler kræver, at der hurtigst muligt foretages en revision af de eksisterende bekendtgørelser, som foreslås videreført i lovforslagets § 55, nr. 2. Der vil således umiddelbart efter en vedtagelse af lovforslaget blive igangsat en gennemgang af de eksisterende bekendtgørelser, hvor der vil ske en inddragelse af de kompetente myndigheder og andre relevante myndigheder, organisationer mv.

For så vidt angår spørgsmålet om forståelsen af begrebet "lov", er Justitsministeriet enig med IT-Politisk Forening i, at der skal være tale om et tilstrækkeligt klart og præcist retsgrundlag for behandling af personoplysninger. Justitsministeriet har derfor præciseret i lovforslagets almindelige bemærkninger, at der skal være tale om tilstrækkeligt klare og præcise regler.

2.2. Lovens anvendelsesområde

Den Uafhængige Politiklagemyndighed bemærker, at det bør være klare, i hvilket omfang politiklagemyndighedens behandling af personoplysninger er omfattet af anvendelsesområdet, herunder i forhold til behandlin-

gen af henholdsvis straffesager efter retsplejelovens kapitel 93 c og adfærdsklagesager efter retsplejelovens kapitel 93 b.

Datatilsynet bemærker, at tilsynet går ud fra, at formuleringen ”automatisk databehandling” i lovforslaget er sammenfaldende med begrebet ”elektronisk databehandling”, som anvendes i persondataloven, men at dette bør præciseres i lovforslaget. Datatilsynet peger endvidere på, at det bør fremgå af lovforslaget, at den behandling af personoplysninger, som finder sted i Hvidvasksekretariatet i Statsadvokaten for Særlig Økonomisk og International Kriminalitet (SØIK) er omfattet af lovforslagets anvendelsesområde.

Rigspolitiet peger på, at lovforslagets bemærkninger bør indeholde en nærmere præcisering af begrebet ”politiaktiviteter, der retter sig mod potentielle strafbare forhold”.

Justitsministeriet er enig med Den Uafhængige Politiklagemyndighed i, at det bør præciseres i lovforslagets almindelige bemærkninger i hvilket omfang politiklagemyndighedens behandling af personoplysninger er omfattet af lovforslagets anvendelsesområde.

Justitsministeriet er endvidere enig med Datatilsynet i, at begrebet ”automatisk databehandling” er sammenfaldende med begrebet ”elektronisk databehandling”, og at det bør fremgå af lovforslagets almindelige bemærkninger, i hvilket omfang den behandling af personoplysninger, som foretages af Hvidvasksekretariatet i Statsadvokaten for Særlig Økonomisk og International Kriminalitet (SØIK), er omfattet af lovforslagets anvendelsesområde.

I forhold til spørgsmålet om lovforslagets anvendelse på politiaktiviteter, der retter sig mod potentielle strafbare forhold, bemærker Justitsministeriet, at det fremgår af pkt. 2.1.3.5 i lovforslagets almindelige bemærkninger, at retshåndhævelsesdirektivet finder 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 di-

rektivet også omfatter udøvelsen af beføjelser gennem tvangsindgreb som f.eks. politiaktiviteter i forbindelse med demonstrationer, store sportsbegivenheder og uroligheder. Disse beføjelser 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.

2.2.1. Statens sikkerhed

Den Uafhængige Politiklagemyndighed bemærker, at lovforslagets § 1, stk. 2, kan give anledning til tvivl i forhold til politiklagemyndighedens behandling af straffesager mod politiansatte hos Politiets Efterretningstjeneste. Politiklagemyndigheden foreslår, at det præciseres, at den behandling af personoplysninger, som foretages af de myndigheder, som efterforsker strafbare forhold vedrørende ansatte i Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste, falder uden for lovens anvendelsesområde.

IT-Politisk Forening anbefaler, at undtagelsen i forhold til national sikkerhed formuleres på samme måde som i retshåndhævelsesdirektivet, dvs. som en undtagelse i forhold til de aktiviteter, som falder uden for EU-rettens anvendelsesområde, i stedet for en generel undtagelse for Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste, idet der henvises til, at efterretningstjenesterne tillige kan behandle personoplysninger til formål, som ikke har forbindelse til den nationale sikkerhed.

Justitsministeriet har foranlediget af høringsvarene fra Den Uafhængige Politiklagemyndighed og IT-Politisk Forening genovervejet spørgsmålet om, hvorvidt der er behov for generelt at undtage den behandling af personoplysninger, som foretages af den militære anklagemyndighed og politiklagemyndigheden i straffesager mod henholdsvis ansatte hos Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste. Det er Justitsministeriet vurdering, at der også i sådanne sager kan være et berettiget hensyn til statens sikkerhed, herunder navnlig for at sikre, at følsomme oplysninger om efterretningstjenesternes forhold ikke kommer til uvedkommendes kendskab. Det er imidlertid Justitsministeriets vurdering, at sådanne hensyn til statens sikkerhed bør varetages på baggrund af en konkret og individuel vurdering, jf. lovforslagets § 14, stk. 1, § 16, stk. 1, og § 17, stk. 5. Justitsministeriet finder på den baggrund ikke, at den militære anklagemyndigheds eller Den Uafhængige Politiklagemyndigheds behandling af

personoplysninger i sager med ansatte fra efterretningstjenester generelt skal være undtaget fra lovens anvendelsesområde.

Justitsministeriet finder omvendt, at den behandling, der foretages af eller for Forsvarets Efterretningstjeneste eller Politiets Efterretningstjeneste, generelt skal være undtaget fra lovens anvendelsesområde, hvilket også er tilfældet i dag.

2.3. Behandlingsregler

IT-Politisk Forening peger på, at lovforslagets bestemmelser om særlige kategorier af oplysninger, hvorefter sådanne oplysninger alene kan behandles, når det er strengt nødvendigt, bør give anledning til en fornyet vurdering af behovet for at behandle f.eks. helbredsoplysninger i Det Centrale Kriminalregister, ligesom behandlingsreglerne i forhold til fingeraftryk og DNA-profiler generelt bør genovervejes.

Justitsministeriet er enig i, at der er behov for at genoverveje reglerne i de eksisterende bekendtgørelser i lyset af lovforslagets og retshåndhævelsesdirektivets regler, jf. også bemærkningerne i pkt. 2.1 ovenfor.

2.4. De registreredes rettigheder

2.4.1. Generelt

IT-Politisk Forening peger på, at der med hjemmel i persondatalovens § 32, stk. 5, er udstedt en række bekendtgørelser, som afskærer de registreredes indsigtret. Retshåndhævelsesdirektivet indeholder efter IT-Politisk Forenings opfattelse en betydelig styrkelse af de registreredes rettigheder, og adgangen til at begrænse de registreredes rettigheder er mere restriktiv end efter gældende ret. IT-Politisk Forening peger også på, at det fremgår af retshåndhævelsesdirektivets præambelbetragtning nr. 44, at den dataansvarlige gennem en konkret og individuel undersøgelse af de enkelte tilfælde skal vurdere, om indsigtretten helt eller delvist skal begrænses. IT-Politisk Forening har forståelse for, at begrænsningerne af retten til indsigt mv. fastsættes i en bekendtgørelse, men finder, at der er behov for en gennemgribende revurdering af de eksisterende begrænsninger af indsigtretten, herunder navnlig i forhold til oplysninger i ANPG-registeret, hvor registreringerne i mange tilfælde ikke er knyttet til konkrete efterforskninger. IT-Politisk Forening bemærker endvidere, at de registreredes ret til be-

rigtigelse mv. alene kan have et reelt indhold, hvis de registrerede kan få indsigt i, hvilke oplysninger der behandles om de pågældende.

Justitsministeriet er enig i, at der er behov for at genoverveje reglerne i de eksisterende bekendtgørelser i lyset af lovforslagets og retshåndhævelsesdirektivets regler, jf. også bemærkningerne i pkt. 2.1 ovenfor.

2.4.2. Adgangen til berigtigelse, sletning og begrænsning af behandling

Datatilsynet peger på, at retshåndhævelsesdirektivets artikel 16, stk. 3, alene giver mulighed for at anvende begrænsning af behandling af personoplysninger i stedet for sletning og ikke – som det fremgår af § 17, stk. 3, i høringsversionen – i stedet for både sletning og berigtigelse.

Rigspolitiet bemærker, at der utilsigtet ses at være skabt en adgang for de registrerede til at gøre sig bekendt med, om de pågældende er undergivet efterforskning af politiet, idet der alene kan gives afslag på indsigt med henvisning til den foreslåede § 16, stk. 3, hvis der rent faktisk behandles oplysninger den pågældende. Den registrerede vil dermed kunne udlede, at den pågældende er undergivet efterforskning og vil have mulighed for at tage sine forholdsregler herimod, hvilket navnlig kan frygtes udnyttet af organiserede kriminelle.

Institut for Menneskerettigheder peger på, at lovforslagets § 14, stk. 1, nr. 5, og § 16, stk. 1, giver mulighed for at indskrænke den registreredes rettigheder af hensyn til den registreredes egne rettigheder. Instituttet finder, at den registreredes indsigtsret er et vigtigt element i den registreredes varetagelse af sine rettigheder, og at disse rettigheder kun bør begrænses i overensstemmelse med retshåndhævelsesdirektivets ordlyd, hvorefter der alene kan ske en begrænsning af hensyn til *andres* rettigheder og frihedsrettigheder.

Justitsministeriet er enig med Datatilsynet i, at retshåndhævelsesdirektivet alene giver mulighed for at anvende begrænsning af oplysninger som et alternativ til sletning. Justitsministeriet har justeret den foreslåede § 17, stk. 3, i overensstemmelse hermed.

Justitsministeriet bemærker i forhold til spørgsmålet om, hvorvidt de registrerede utilsigtet kan få adgang til oplysninger om, hvorvidt der behandles oplysninger om de pågældende, at der med den foreslåede ordning fortsat vil være mulighed for, at politiet – når indsigtsretten er afskåret –

generelt orienterer de registrerede om, at der ikke kan opnås indsigt i de pågældende oplysninger, uanset om der konkret behandles oplysninger om den pågældende eller ej. Justitsministeriet finder på den baggrund ikke, at der med den foreslåede ordning kan ske en utilsigtet afsløring af, at den pågældende er undergivet efterforskning af politiet. Justitsministeriet bemærker dog i den forbindelse, at der som nævnt oven for i pkt. 2.1 er behov for at genoverveje reglerne i de eksisterende bekendtgørelser i lyset af lovforslagets og retshåndhævelsesdirektivets regler.

Justitsministeriet finder, at hensynet til den registrerede selv fortsat bør kunne føre til, at der sker en begrænsning af den registreredes rettigheder, idet der navnlig på kriminalforsorgens område kan være tale om et meget tungtvejende hensyn til registrerede, som befinder sig i psykisk sårbare situationer. Hertil kommer, at den registrerede under alle omstændigheder vil have mulighed for at udøve sine rettigheder gennem tilsynsmyndigheden, jf. den foreslåede § 40, stk. 1, nr. 10.

2.4.3. Samspelet mellem lovforslaget og retsplejeloven

Datatilsynet peger på, at der er en ikke ubetydelig del af straffesagerne, som ikke vil blive underlagt domstolsprøvelse, og at den registrerede derfor ikke ad rettens vej vil få mulighed for at få berigtiget eventuelle urigtige oplysninger.

Rigsadvokaten peger på, at retsplejeloven indeholder en række regler om bl.a. adgang til det materiale, som indgår i konkrete straffesager, og om indsigt i og berigtigelse af retsafgørelser. Det er derfor væsentligt, at der i lovforslaget tages nærmere stilling til forholdet mellem de foreslåede regler og retsplejeloven.

Justitsministeriet har foranlediget af høringsssvarene fra Datatilsynet og Rigsadvokaten genovervejet spørgsmålet om forholdet mellem lovforslagets og retsplejelovens regler om udøvelsen af de registreredes rettigheder. Justitsministeriet finder, at oplysningspligten over for den registrerede samt anmodninger om indsigt, berigtigelse, sletning eller begrænsning af behandling af personoplysninger generelt bør håndteres efter retsplejelovens regler, i det omfang retsplejelovens regler finder anvendelse. Hertil kommer, at retsplejelovens regler suppleres af den militære retsplejelov, for så vidt angår militære straffesager, hvilket indebærer, at der i sådanne sager tillige vil kunne ske en begrænsning af den registreredes rettigheder med henvisning til den militære sikkerhed. Den foreslåede § 18, stk. 3, er

på den baggrund justeret, således at retsplejelovens og den militære retsplejelovs regler om retten til oplysninger, indsigt i og berigtigelse eller sletning og begrænsning af behandling af personoplysninger i straffesager finder anvendelse i forhold til den registrerede. For så vidt angår registrerede, hvis indsigtsret ikke er reguleret af retsplejelovens regler, f.eks. personer, som optræder som bipersoner i en straffesag, indebærer den foreslåede ordning, at der i sådanne situationer faldes tilbage på lovforslagets regler.

2.4.1. Sondring mellem forskellige kategorier af registrerede

Datatilsynet peger på, at der kan være behov for at tage stilling til, hvordan de kompetente myndigheder skal behandle oplysninger om personer, som på samme tid kan kategoriseres som både ofre og sigtede eller mistænkte.

IT-Politisk Forening peger på, at navnlig ANPG-systemet i dag behandler oplysninger om personer, som ikke mistænkt for strafbare forhold, og at der er behov for en særlig beskyttelse af sådanne registrerede.

Som anført i pkt. 2.3.3.3 i lovforslagets almindelige bemærkninger indeholder retshåndhævelsesdirektivets artikel 6 og artikel 7, stk. 1, 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 behandlingskravene. 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 kan være behov for, at de kompetente myndigheder, inden en konkret behandling iværksættes, inddrager spørgsmålet om, hvilken kategori en registreret person tilhører.

Justitsministeriet er herudover enig i, at der er behov for at genoverveje reglerne i de eksisterende bekendtgørelser i lyset af lovforslagets og retshåndhævelsesdirektivets regler, herunder for fortsat at understøtte, at der sker en differentieret behandling af oplysninger om forskellige kategorier af registrerede, jf. også bemærkningerne i pkt. 2.1 ovenfor.

2.5. Forpligtelser for den dataansvarlige og databehandleren

2.5.1. Generelt

Datatilsynet peger på, at der i lovforslagets bemærkninger bør gives eksempler på, hvordan den dataansvarlige kan påse, at databehandleren træffer de fornødne tekniske og organisatoriske foranstaltninger, f.eks. gennem indhentelse af uvildige revisionserklæringer, fysisk besøg hos databehandleren eller en procedure for kontinuerligt tjek af databehandlerens persondatasikkerhedspolitikker.

Justitsministeriet er enig med Datatilsynet i, at det er hensigtsmæssigt, at det fremgår af lovforslagets almindelige bemærkninger, hvordan de dataansvarlige myndigheder kan påse, at databehandlere træffer de fornødne tekniske og organisatoriske foranstaltninger. Justitsministeriet har præciseret de specielle bemærkninger til lovforslagets § 22 i overensstemmelse hermed.

2.5.2. Fælles dataansvarlige

Rigspolitiet peger på, at der med fordel kan etableres hjemmel til generelt at fastsætte nærmere regler om, hvortil den registrerede skal rette sin anmodning om udøvelse af sine rettigheder, samt om behandlingen af sådanne anmodninger. Rigspolitiet foreslår endvidere, at det overvejes, om der bør fastsættes en hjemmel til at regulere klageadgangen i forhold til de afgørelser, som træffes i forbindelse med de registreredes udøvelse af sine rettigheder efter loven.

Justitsministeriet er enig med Rigspolitiet i, at der med fordel kan indsættes en bemyndigelse til justitsministeren til at fastsætte nærmere regler om, hvortil en registreret skal rette sin anmodning om f.eks. indsigt eller berigtigelse af oplysninger og om adgangen til at påklage afgørelser, som træffes i forbindelse med de registreredes udøvelse af deres rettigheder efter loven. Justitsministeriet har på den baggrund tilføjet et nyt stk. 4 til lovforslagets § 18.

2.5.3. Databeskyttelse gennem design og standardindstillinger

Datatilsynet og IT-Politisk Forening finder, at kravet om, at de fornødne tekniske og organisatoriske foranstaltninger kan bestå af databeskyttelse gennem design eller standardindstillinger ikke kun er relevant i forhold til

fremtidige systemer, men at kravet tillige bør finde anvendelse ved væsentlige ændringer af behandlingen af oplysninger i eksisterende systemer.

Justitsministeriet er enig med Datatilsynet og IT-Politisk Forening i, at kravet om databeskyttelse gennem design og standardindstillinger ikke er begrænset til nye systemer. Justitsministeriet har på den baggrund slettet lovforslagets § 53, stk. 2, ligesom det er præciseret i de specielle bemærkninger til lovforslagets § 20, at kravet om databeskyttelse gennem design og standardindstillinger tillige finder anvendelse i forhold til væsentlige ændringer i behandlingen af oplysninger i eksisterende systemer.

2.5.4. Fortegnelser

IT-Politisk Forening bemærker, at det fremgår af lovforslaget, at kravene til indholdet af de fortegnelser over behandlingsaktiviteter, som de dataansvarlige skal føre, svarer til indholdet af de anmeldelser, som efter gældende ret skal indgives til Datatilsynet. IT-Politisk Forening bemærker herom, at anmeldelser efter persondataloven i dag findes på Datatilsynets hjemmeside, uanset at dette ikke er et krav efter persondataloven, og at der derfor opfordres til, at fortegnelser over behandlingsaktiviteter på tilsvarende måde gøres offentligt tilgængelige på enten den dataansvarliges eller Datatilsynets hjemmeside, da dette er et nyttigt arbejdsredskab for bl.a. IT-Politisk Forening, ligesom det kan styrke offentlighedens tillid til den offentlige sektors, herunder de retshåndhævende myndigheders, behandling af personoplysninger.

Det fremgår af persondatalovens § 54, stk. 1, at tilsynsmyndigheden skal føre en fortegnelse over de behandlinger, der er anmeldt efter persondatalovens §§ 43, 48 og 52. Fortegnelsen, som mindst skal indeholde de oplysninger, som er anført i persondatalovens § 43, stk. 2, skal være tilgængelig for offentligheden. Persondatalovens § 54, stk. 1, har sin baggrund i databeskyttelsesdirektivets artikel 21, stk. 2. Retshåndhævelsesdirektivet indeholder imidlertid ikke et tilsvarende krav om, at fortegnelser skal stilles til rådighed for offentligheden. Justitsministeriet finder på den baggrund ikke, at der er behov for at indsætte et krav om, at fortegnelserne skal stilles til rådighed for offentligheden.

2.5.5. Logningskravet

Datatilsynet peger på, at der mangler en eksplicit bestemmelse om udskudt ikrafttrædelsestidspunkt for lovforslagets § 24 om logning.

IT-Politisk Forening peger på, at retshåndhævelsesdirektivets artikel 63 alene giver mulighed for at udskyde anvendelsestidspunktet for logningskravet i forhold til automatiske databehandlingssystemer, der er indført før den 6. maj 2016.

Domstolsstyrelsen noterer sig, at lovforslagets § 24, stk. 2, indeholder en bemyndigelse for justitsministeren til at fastsætte nærmere regler om, hvilke automatiske databehandlingssystemer som logningskravet finder anvendelse på.

Justitsministeriet er enig med IT-Politisk Forening i, at retshåndhævelsesdirektivets artikel 63 alene giver mulighed for at udskyde anvendelsestidspunktet for logningskravet i forhold til automatiske databehandlingssystemer, der er indført før den 6. maj 2016. Lovforslagets § 24, stk. 2, er justeret i overensstemmelse hermed.

2.5.5. Forudgående høring af tilsynsmyndighederne

Datatilsynet finder, at kravet om, at der skal foretages forudgående høring af tilsynsmyndighederne, skal knyttes til nye og væsentlig ændrede behandlinger, som medfører en (fornyet) høj risiko for fysiske personers rettigheder, uanset om dette foretages i allerede etablerede systemer.

Det fremgår af retshåndhævelsesdirektivets artikel 28, stk. 1, at medlemsstaterne fastsætter bestemmelser om, at den dataansvarlige eller databehandleren i visse situationer skal høre tilsynsmyndigheden inden behandling af personoplysninger, der vil indgå som en del af et nyt register, der skal oprettes. Justitsministeriet finder på den baggrund, at lovforslagets krav om forudgående høring på tilsvarende vis skal angå nye registre, der oprettes.

2.5.6. Brud på datasikkerheden

IT-Politisk Forening noterer sig, at reglerne om behandling af oplysninger om personnummer ikke videreføres i lovforslaget, men anbefaler, at det angives i bemærkningerne, at et brud på datasikkerheden, som omfatter

oplysninger om personnummer, bør føre til, at der sker en underretning af de registrerede.

Justitsministeriet er enig med IT-Politisk Forening i, at et brud på datasikkerhed, som omfatter oplysninger om personnummer, bør føre til, at der sker en underretning af de registrerede. Det er på den baggrund præciseret i de specielle bemærkninger til lovforslagets § 29, at det f.eks. vil være relevant for den dataansvarlige at foretage underretning af en registreret, hvis bruddet på persondatasikkerheden har ført til, at oplysninger om den registreredes personnummer kan være kommet til uvedkommendes kendskab.

2.6. Tilsynsmyndighederne

2.6.1. Generelt

Datatilsynet foreslår, at lovforslagets § 40, stk. 2, omformuleres til følgende ordlyd: ”Tilsynsmyndighederne letter indgivelse af klager efter stk. 1, nr. 6.”. Datatilsynet forudsætter herudover at blive hørt over eventuelle bekendtgørelser, der udstedes i medfør af loven.

Justitsministeriet er enig med Datatilsynet i, at lovforslagets § 40, stk. 2, med fordel kan formuleres i overensstemmelse med Datatilsynets forslag. Lovforslagets § 40, stk. 2, er således justeret i overensstemmelse hermed.

Det fremgår af lovforslagets § 43, at ved udarbejdelse af generelle retsfor skrifter, der har betydning for behandling af personoplysninger, skal der indhentes en udtalelse fra Datatilsynet. Er der tale om generelle forskrifter, der har betydning for behandling af oplysninger, der foretages for domstolene, skal der indhentes en udtalelse fra Domstolsstyrelsen.

2.6.2. Indberetning af overtrædelser af loven

Datatilsynet er uforstående over for den foreslåede bestemmelse i lovforslagets § 12, idet Datatilsynet finder, at indberetning bør kunne ske til f.eks. databeskyttelsesrådgiveren.

Det fremgår af retshåndhævelsesdirektivets artikel 48, at medlemsstaterne fastsætter bestemmelser om, at de kompetente myndigheder skal indføre effektive mekanismer, som tilskynder til fortrolig indberetning af overtrædelser af direktivet. Direktivets artikel 48 er placeret i direktivets kapitel VI

om uafhængige tilsynsmyndigheder, og det er på den baggrund Justitsministeriets vurdering, at bestemmelsen vedrører indberetning til tilsynsmyndigheden og ikke – som foreslået af Datatilsynet – til f.eks. en databeskyttelsesrådgiver.

2.6.3. Tilsynsmyndighedernes adgang til oplysninger

Datatilsynet finder, at det bør fremgå eksplicit af lovforslaget, at fortegnelser over behandlingsaktiviteter og dokumentation for brud på datasikkerheden skal stilles til rådighed for tilsynsmyndighederne. Datatilsynet finder endvidere, at der bør fastsættes en nærmere angivet opbevaringsperiode, f.eks. mindst fem år, for dokumentation for sikkerhedsbrud.

Det fremgår af lovforslagets § 41, 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. Tilsynsmyndighederne vil således på grundlag af denne bestemmelse kunne kræve, at fortegnelser over behandlingsaktiviteter og dokumentation for brud på datasikkerheden stilles til rådighed.

Justitsministeriet finder ikke, at der er behov for, at der i loven fastsættes en nærmere angivet opbevaringsperiode, f.eks. mindst fem år, for dokumentation for sikkerhedsbrud. Spørgsmålet om, hvor længe de dataansvarlige myndigheder skal opbevare dokumentationen, afhænger således af en konkret vurdering af bl.a. karakteren og omfanget af den behandling af personoplysninger, som den pågældende myndighed foretager. Det vil være op til tilsynsmyndighederne at fastsætte nærmere retningslinjer for, hvor længe dokumentation skal opbevares.

2.7. Retsmidler og erstatning

Institut for Menneskerettigheder finder, at der ikke foreligger særlige grunde til at ændre på den gældende retstilstand i forhold til erstatning, hvorefter der gælder et skærpet ansvarsgrundlag i form af et præsump-tionsansvar. Instituttet anbefaler derfor, at der sker en videreførelse af ordningen med et præsump-tionsansvar, uanset at retshåndhævelsesdirektivet ikke stiller krav herom.

Justitsministeriet har foranlediget af høringssvaret fra Institut for Menneskerettigheder genovervejet spørgsmålet om, hvordan reglerne om erstatning for overtrædelser af loven skal udformes. Som anført af Institut for

Menneskerettigheder gælder der i dag et skærpet ansvarsgrundlag i form af et præsumptionsansvar (culpa med omvendt bevisbyrde). Som det fremgår af pkt. 2.10.3.5 i lovforslagets almindelige bemærkninger, fremgår det af forarbejderne til persondataloven, 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. Det følger imidlertid af praksis fra EU-Domstolen, at spørgsmål om EU-medlemsstaternes erstatningsansvar for tilsidesættelse af EU-retten skal håndteres i medfør af de almindelige regler om EU-medlemsstaternes erstatningsansvar. Der er på den baggrund ikke grundlag for at fastsætte en ordning med et skærpet ansvarsgrundlag i form af et præsumptionsansvar.

3. Lovforslaget

I forhold til lovudkastet, der har været sendt i høring, er der foretaget følgende indholdsmæssige ændringer:

1. Det foreslås, at lovforslagets § 1 om anvendelsesområdet for lovforslaget justeres, således at den behandling af personoplysninger, som foretages af militærpolitiet, ikke længere er omfattet.
2. Det er præciseret i de specielle bemærkninger til lovforslagets § 1, at begrebet automatisk databehandling er sammenfaldende med elektronisk databehandling, som anvendes i persondatalovens § 1, stk. 1.
3. Der er indsat en kort beskrivelse af retsplejelovens kapitel 93 c om behandlingen af straffesager mod politipersonale i pkt. 1.3.3 i lovforslagets almindelige bemærkninger.
4. Der er endvidere i pkt. 2.1.3.5 i lovforslagets almindelige bemærkninger indsat en præcisering af lovforslagets anvendelse for den behandling af personoplysninger, som foretages af Den Uafhængige Politiklagemyndigheds og Hvidvasksekretariatet i Statsadvokaten for Særlig Økonomisk og International Kriminalitet (SØIK).
5. Det er præciseret i pkt. 2.3.3.1 i lovforslagets almindelige bemærkninger, at begrebet "lov" vil i denne forbindelse omfatte enhver eksisterende

regulering, der på den fornødne klare og præcise måde generelt eller konkret hjemler, at behandling kan finde sted.

6. Det er præciseret i pkt. 2.3.3.5 og 2.3.3.6 i lovforslagets almindelige bemærkninger, hvordan den behandling, som hidtil er foretaget på grundlag af et samtykke fra den registrerede, jf. persondatelovens § 6, stk. 1, nr. 1, fremover kan ske i medfør af lovforslagets §§ 8 og 10.

7. Der er i de specielle bemærkninger til lovforslagets § 1, stk. 2, og § 14 sket en præcisering af spørgsmålet om varetagelsen af hensynet til statens sikkerhed.

Henvisningen til den behandling, som foretages af den militære anklagemyndighed i forbindelse med sager mod ansatte fra Forsvarets Efterretningstjeneste, er således slettet fra de specielle bemærkninger til lovforslagets § 1, stk. 2,

På den anden side er det præciseret i de specielle bemærkninger til lovforslagets § 14, at hensynet til statens sikkerhed, herunder den militære sikkerhed, f.eks. kan være relevant i forbindelse med de kompetente myndigheders behandling af sager mod ansatte fra Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste.

8. Det foreslås, at lovforslagets § 17, stk. 3, justeres, således at der kan ske begrænsning af behandling af personoplysninger i stedet for sletning (men ikke berigtigelse).

9. Det foreslås, at lovforslagets § 18, stk. 3, justeres, således at retsplejelovens og den militære retsplejelovs regler om retten til oplysninger, indsigt i og berigtigelse eller sletning og begrænsning af behandling af personoplysninger i straffesager finder anvendelse i forhold til den registreredes rettigheder i medfør af lovforslagets afsnit III.

10. Det foreslås, at der tilføjes et nyt stykke 4 til lovforslagets § 18, hvor justitsministeren bemyndiges til at fastsætte nærmere regler om behandling af anmodninger i medfør af lovforslagets afsnit III samt om behandling af klagesager, herunder at afgørelser ikke skal kunne påklages til anden administrativ myndighed.

11. I de specielle bemærkninger til lovforslagets § 22 er der sket en eksemplificering af, hvordan den dataansvarlige kan påse, at databehandlere har truffet de fornødne foranstaltninger.

12. Det foreslås, at lovforslagets § 24, stk. 2, om anvendelsestidspunktet for logningskravet justeres, således at justitsministeren bemyndiges til at fastsætte nærmere regler om anvendelsestidspunktet for logningskravet i forhold til automatiske databehandlingssystemer, som er indført før den 6. maj 2016.

13. I de specielle bemærkninger til lovforslagets § 29 er der sket en eksemplificering af, at der skal ske underretning af registrerede ved brud på datasikkerheden, som fører til, at uvedkommende kan få kendskab til oplysninger om de pågældendes personnummer.

14. Det foreslås, at lovforslagets § 40, stk. 2, justeres, således at tilsynsmyndighederne skal lette indgivelsen af klager efter stk. 1, nr. 6. I høringsversionen var det et krav, at tilsynsmyndighederne skulle fastsætte nærmere regler herom.

15. Det foreslås, at lovforslagets § 46 om erstatning justeres, således at spørgsmål om erstatning skal afgøres efter det almindelige EU-retlige erstatningsansvar.

16. Det er i pkt. 2.8.3 i lovforslagets almindelige bemærkninger præciseret, hvilke regler der gælder for de danske myndigheders videregivelse af oplysninger til Europol.

17. Lovforslagets § 53, stk. 2, om anvendelsen af kravet om databeskyttelse gennem design og standardindstillinger i § 20 er slettet, ligesom det er præciseret i de specielle bemærkninger til lovforslagets § 20, at kravet om databeskyttelse gennem design og standardindstillinger tillige finder anvendelse ved væsentlige ændringer i behandlingen af oplysninger i eksisterende systemer.

18. Der er indsat tekst i pkt. 3 i lovforslagets almindelige bemærkninger om de økonomiske og administrative konsekvenser for det offentlige.

19. Der er indsat tekst i pkt. 5 i lovforslagets almindelige bemærkninger om de administrative konsekvenser for borgerne.

Der er herudover foretaget en række redaktionelle ændringer og præcisering i forhold til det lovudkast, der har været sendt i høring, herunder mindre ændringer af sproglig og lovteknisk karakter.