Københavns Byret

Justitsministeriet
Slotsholmsgade 10
1260 København K

Præsidenten
Domhuset, Nytorv 25
1450 København K.
Tlf. 99 68 70 15
CVR 21 65 95 09
administration.kbh@domstol.dk
J. nr. 9099.2017.21

Den 21. marts 2017

Ved en mail af 1. marts 2017 har Justitsministeriet anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger.

Jeg skal i den anledning oplyse, at Københavns Byret kan henholde sig til det af Østre Landsret anførte.

Der henvises til J.nr. 2016-7910-0008.

Med venlig hilsen

Søren Axelsen

DEN
UAFHÆNGIGE
POLITIKLAGEMYNDIGHED

Justitsministeriet
Slotsholmsgade 10
1216 København K

Digital post: jm@jm.dk

Høringssvar vedrørende forslag til lov om retshåndhævende myndigheders behandling af personoplysninger

Aarhus, 6. marts 2017

Journalnr.: DUP-2017-149-0022

Sekretær: Allan Knudsen
Sagsbehandler: Cecilie Revsbech

Justitsministeriet har ved brev af 1. marts 2017 anmodet om Den Uafhængige Politiklagemyndigheds (Politiklagemyndigheds) bemærkninger til lovforslaget.

Desuden har ministeriet ved e-mail af 24. februar 2017 anmodet Politiklagemyndigheden om et skøn over de økonomiske konsekvenser af lovforslaget for myndigheden.

Politiklagemyndigheden har gennemgået lovforslaget og skal bemærke følgende:

1. I lovforslagets almindelige bemærkninger, afsnit 2.1.3.5 (s. 42) og de specielle bemærkninger til § 1, stk. 1 (s. 121) vedrørende lovens anvendelsesområde, bør der efter Politiklagemyndighedens opfattelse indsættes et afsnit om Politiklagemyndighedens kompetence, herunder sondringen mellem straffesager (rpl. kap. 93 c) og adfærdsklagesager (rpl. kap. 93 b).

2. Det er Politiklagemyndighedens opfattelse, at lovforslagets § 1, stk. 2, kan give anledning til fortolkningstvivl for så vidt angår lovens anvendelsesområde i forhold til Politiklagemyndighedens behandling af straffesager mod politiansatte hos PET.

Politiklagemyndigheden foreslår på den baggrund, at følgende tilføjes til ordlyden af bestemmelsen: "eller den behandling af personoplysninger, som udføres af myndigheder, som efterforsker strafbare forhold vedrørende ansatte i disse tjenester." Under alle omstændigheder bør det præciseres i forarbejderne, at Politiklagemyndighedens efterforskning i straffesager mod PET-ansatte falder uden for lovens anvendelsesområde, jf. de almindelige bemærkninger afsnit 2.1.3.6 (s. 45) og de specielle bemærkninger til lovens § 1, stk. 2 (s. 124), hvor den militære anklagemyndighed er omtalt.

3. I lovforslagets almindelige bemærkninger, afsnit 1.3.3 (s. 34) bør der efter Politiklagemyndighedens opfattelse indsættes en kort beskrivelse af retsplejelovens kap. 93 c (straffesager mod politipersonale).

4. Det er Politiklagemyndighedens opfattelse, at Politiklagemyndigheden også bør omtales de steder i forarbejderne, hvor der er henvist til politi og anklagemyndighed, f.eks. de specielle bemærkninger til lovens § 1, stk. 1 (s. 123, afsnit 3) og § 4, stk. 8 (s. 139).

5. Endelig er det Politiklagemyndighedens vurdering, at implementeringen af lovforslaget vil indebære øgede lønomkostninger for myndigheden, herunder til en databeskyttelsesrådgiver, svarende til i første omgang anslået én ekstra administrativ medarbejder (1 årsværk).

Med venlig hilsen

Kirsten Dyrman
direktør

Domstolsstyrelsen

Justitsministeriet
Slotsholmsgade 10
1216 København K

Store Kongensgade 1-3
1264 København K
Tlf. +45 70 10 33 22
post@domstolsstyrelsen.dk
CVR-nr. 21659509
EAN-nr. 5798000161184

J.nr.: 2017-3302-0001-30
Sagsbehandler: Maiken Michelsen
Mail: MIMI@domstolsstyrelsen.dk
16. marts 2017

Domstolsstyrelsens høringssvar vedrørende forslag til lov om retshåndhævende myndigheders behandling af personoplysninger (gennemførelse af direktiv om databeskyttelse på retshåndhævelsesområdet)

Domstolsstyrelsen har modtaget Justitsministeriets udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger (gennemførelse af direktiv om databeskyttelse på retshåndhævelsesområdet).

Domstolsstyrelsen har følgende bemærkninger:

Det vil efter Domstolsstyrelsen vurdering ikke være muligt at iagttage lovforslagets § 24, stk. 1, om at der i automatiske databehandlingssystemer (skal) foretages logning af indsamling, ændring, videregivelse, herunder overførsel, samkøring og sletning, i tilknytning til lovforslagets foreslåede tidspunkt for ikrafttræden. Domstolsstyrelsen har derfor noteret, at det af lovforslagets § 24, stk. 2, fremgår, at justitsministeren får bemyndigelse til at fastsætte nærmere regler om, hvilke automatiske databehandlingssystemer logningskravet skal finde anvendelse på, og at det af bemærkningerne til bestemmelsen bl.a. fremgår, at denne ordning giver mulighed for, at der sammen med de kompetente myndigheder kan ske en nærmere afklaring af rækkevidden af logningsforpligtelsen, samt at der er mulighed for en løbende indfasning af forpligtelsen.

Der henvises i øvrigt til Domstolsstyrelsens høringssvar af 9. marts 2017 vedrørende de økonomiske konsekvenser ved udkastet til lovforslaget.

Med venlig hilsen

Laila Lindemark

Justitsministeriet
Lovafdelingen
Databeskyttelseskontoret
Slotsholmsgade 10
1216 København K

RIGSADVOKATEN

RIGSADVOKATEN
FREDERIKSHOLMS KANAL 16
1220 KØBENHAVN K

TELEFON: 7268 9000
FAX: 7268 9004
E-MAIL: RIGSADVOKATEN@ANKL.DK
www.anklagemyndigheden.dk

DATO 15. marts 2017

JOURNAL NR.
RA-2017-3200601-1

SAGSBEHANDLER: JSB/

Høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger

Ved e-mail af 1. marts 2017 (sagsnr. 2016-7910-0008) har Justitsministeriet anmodet om Rigsadvokatens eventuelle bemærkninger til udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger (gennemførelse af direktiv om databeskyttelse på retshåndhævelsesområdet).

Med lovudkastet foreslås en ny hovedlov om behandling af personoplysninger i bl.a. politiet og anklagemyndigheden. Lovudkastet tager sigte på at gennemføre Europa-Parlamentets og Rådets direktiv 2016/680/EU af 27. april 2016 (retshåndhævelsesdirektivet) i dansk ret.

Jeg skal bemærke, 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 efter min opfattelse væsentligt, at der i lovudkastet tages nærmere stilling til forholdet mellem de foreslåede regler og de eksisterende bestemmelser i retsplejeloven. Jeg henviser i den forbindelse også til direktivets artikel 18 om anvendelse af nationale retsplejeregler.

Jeg skal endvidere bemærke, at implementeringen af direktivet - ud over udgifter knyttet til den it-tekniske opfølgning - også vil kunne indebære, at der skal varetages en række nye opgaver med hensyn til håndtering af underretningspligt, indsigtsret, databeskyttelsesrådgiver mv. Det er ikke på det foreliggende grundlag muligt at skønne

over ressourcerne hertil, men afhængig af hvordan opgavevaretagelsen på de relevante områder nærmere tilrettelægges, må disse opgaver også forventes at kunne indebære en betydelig ressourceanvendelse.

Med venlig hilsen

Jens Røn
Statsadvokat

RIGSPOLITIET

POLITI

Justitsministeriet
Databeskyttelseskontoret

Sendt til:
databeskyttelseskontoret@jm.dk,
kra@jm.dk

Den 15. marts 2017
Sagsbehandler: jha
J.nr. 2017-6140-1

POLITIOMRÅDET

Forretningsudvikling
Databeskyttelsesenheden
Polititorvet 14
1780 København V

Telefon: 33 14 88 88

E-mail: politi@politi.dk
Web: www.politi.dk

Vedrørende høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger.

Justitsministeriet har ved brev af 1. marts 2017 anmodet om bemærkninger til udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger.

Generelle bemærkninger

I forlængelse af Rigspolitiets tidligere afgivne høringssvar vedrørende EU's direktiv om databeskyttelse på retshåndhævelsesområdet, herunder senest høringssvaret af 23. september 2016 i anledning af forslag til folketingsbeslutning om Danmarks tilslutning til direktivet på mellemfolkeligt grundlag, skal det generelt bemærkes, at implementeringen af loven vil være forbundet med ikke-ubetydelige personale-, samt system- og IT-mæssige omkostninger for politiet.

Det bemærkes endvidere, at den fremrykkede implementering af direktivet og den korte frist, som dansk politi vil have til at indrette sig på lovens endelige indhold, må forventes at indebære visse udfordringer.

Rigspolitiet har noteret 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.

Rigspolitiet skal i øvrigt bemærke følgende:

Lovens anvendelsesområde

Det fremgår af de almindelige bemærkninger til lovforslagets § 1, at direktivet også omfatter politiaktiviteter, der retter sig mod potentielle strafbare forhold. Det fremgår videre af de almindelige bemærkninger, at spørgsmålet om rækkevidden af direktivets anvendelsesområde i forhold til politiets opgaver forbundet med opretholdelse af lov og orden vil skulle fastlægges nærmere i praksis.

Det er Rigspolitiets opfattelse, at det ville være hensigtsmæssigt i bemærkningerne at foretage en nærmere præcisering af rækkevidden af begrebet "politiaktiviteter, der retter sig mod potentielle strafbare forhold". Det fremstår således uklart om eksempelvis politiets opgaver i forbindelse med udstedelse af zoneforbud i medfør af ordensbekendtgørelsen, afgørelser truffet i medfør af lov om tilhold, opholdsforbud og bortvisning og restaurationsloven, beslutning om indførelse af visitationszoner i medfør af politiloven, inddragelse af pas og opholdstilladelse efter pasloven, udlændingeloven og retsplejeloven mv. vil være omfattet af lovens anvendelsesområde.

Såvel de almindelige som de specielle bemærkninger henviser til ordlyden af direktivets præambelbetragtning nr. 12 om politiaktiviteter i forbindelse med demonstrationer, store sportsbegivenheder og uroligheder som eksempler på tilfælde, hvor direktivet omfatter udøvelsen af beføjelser gennem tvangsindgreb. De pågældende eksempler synes umiddelbart udelukkende at omfatte større begivenheder svarende til offentlige forsamlinger og opløb, jf. herved politilovens §§ 7-9.

Rigspolitiet skal foreslå, at det præciseres, at tvangsindgreb omfattet af direktivet omfatter ethvert tvangsindgreb, der gennemføres af politiet.

Rigspolitiet skal endvidere foreslå, at det i lovens bemærkninger præciseres, at også politiets arbejde efter politilovens §§ 5-6 vil være omfattet af loven og dermed falde uden for anvendelsesområdet for databeskyttelsesforordningen, der træder i kraft den 25. maj 2018.

Oplysningspligt

Lovforslagets § 13 indeholder skærpede krav til oplysningspligten. Dataansvarlige skal således stille de i § 13, stk. 1, anførte oplysninger til rådighed for den registrerede og, hvor det er nødvendigt for at registrerede kan varetage sine interesser, skal dataansvarlige endvidere, i konkrete sager, som minimum stille en række yderligere oplysninger til rådighed for den registrerede jf. § 13, stk. 2.

Lovforslagets § 14, stk. 2, indeholder en bemyndigelse for Justitsministeren til at fastsætte nærmere regler om udsættelse, begrænsning eller undladelse af oplysningspligten.

En nærmere vurdering af oplysningspligtens omfang vil i høj grad afhænge af den nærmere fortolkning af rækkevidden af § 13, stk. 2, samt de nærmere regler, der er hjemmel til at fastsætte i medfør af § 14, stk. 2. Rigspolitiet har i den forbindelse noteret sig, at det fremgår af de specielle bemærkninger til § 14, stk. 2, at der i videst muligt omfang vil kunne fastsættes regler om, at meddelelse bør finde sted samtidig med de øvrige processuelle skridt, som straffesager er underlagt.

Indsigtsret

Rigspolitiet skal bemærke, at der med de i lovforslagets § 16, stk. 2 og 3, hjemlede undtagelser til indsigtsretten umiddelbart synes at være skabt en utilsigtet adgang for de registrerede til at gøre sig bekendt med, om de pågældende er undergivet efterforskning af politiet.

Det vil således umiddelbart kun være relevant at give afslag på indsigt i medfør af bestemmelsen i lovforslagets § 16, stk. 3, i de tilfælde, hvor der på tidspunktet for afgivelsen af anmodningen om indsigt behandles oplysninger om den registrerede. Herved vil eksempelvis mistænkte have mulighed for at kunne udlede, at de er undergivet efterforskning og tage forholdsregler for at imødegå politiets efterforskning mv., hvilket navnlig kan frygtes udnyttet af organiserede kriminelle.

Rigspolitiet opfordrer på den baggrund til, at der i lovforslaget tages stilling til, hvordan denne problemstilling bedst adresseres, herunder om Rigspolitiets praksis i forhold til indsigt i bl.a. PED mere generelt bør afspejles i lovforslaget.

Det bør endvidere i forbindelse med reguleringen af adgangen til at fastsætte regler i medfør af § 16, stk. 4, overvejes, om der i praksis bør være en grundlæggende afstemning mellem de tilfælde, hvor der gøres undtagelser for oplysningspligten, og i hvilket omfang adgangen til indsigt er afskåret efter disse regler.

Fælles dataansvarlige

Det fremgår af lovforslagets § 21, at 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, som bl.a. skal omfatte udpegningen af et fælles kontaktpunkt.

I lovforslagets almindelige bemærkninger redegøres der for Datatilsynets hidtidige praksis i forhold til fælles dataansvar, herunder at tilsynet har krævet, at registrerede skal kunne gøre deres rettigheder efter persondatalovens afsnit III, såsom retten til indsigt, oplysninger mv., gældende over for enhver af de fælles dataansvarlige.

Rigspolitiet finder bl.a. på den baggrund, 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 heraf. Det kan endvidere overvejes, om der tillige bør fastsættes en hjemmel til at regulere klageadgangen i forhold til de afgørelser, der træffes i forbindelse med den registreredes udøvelse af sine rettigheder efter loven.

Der henvises til Justitsministeriets j.nr. 2016-7910-0008.

Med venlig hilsen

Svend Larsen
politidirektør

Kenny Rasmussen

Fra: Marie Granborg [MGr@skm.dk]
Sendt: 15. marts 2017 14:02
Til: #951dep-Databeskyttelseskontoret; Kenny Rasmussen
Cc: Stine Hindsgaul Hansen
Emne: Høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger - (2016-7910-0008)
Vedhæftede filer: Forslag til lov om retshåndhævende myndigheders behandling af personoplysninger [DOK2229227].pdf; Høringsliste [DOK2228621].pdf; Bilag - Retshåndhævelsesdirektivet.pdf; fesdPacket.xml; Høringsbrev [DOK2228666].pdf

Kære Kenny

Skatteministeriet har modtaget høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger. Skatteministeriet har ingen bemærkninger til lovforslaget.

Mvh Marie

Med venlig hilsen

Marie Granborg
Fuldmægtig, jurist
Implementeringsprogram
Kommunikation og Lokalisering

Tel. +45 72 38 41 97
Mail MGR@skm.dk

Skatteministeriet

Skatteministeriet/Ministry of Taxation
Nicolai Eigtveds Gade 28
DK 1402 - København K

Mail skm@skm.dk
Web www.skm.dk

Fra: Justitsministeriet [mailto:jm@jm.dk]
Sendt: 1. marts 2017 16:10
Til: samfund@advokatsamfundet.dk; mail@danskeadvokater.dk; dt@datatilsynet.dk; mikaelsjoeberg@oestrelandsret.dk; $Direktoratet for Kriminalforsorgen; hoeringer@dommerfm.dk; post@domstolsstyrelsen.dk; lsc@ankl.dk; info@humanrights.dk; kobenhavn@domstol.dk; pt@strafferetsadvokaten.dk; mail@politiforbundet.dk; aalborg@domstol.dk; aarhus@domstol.dk; esbjerg@domstol.dk; glostrup@domstol.dk; helsingor@domstol.dk; herning@domstol.dk; hillerod@domstol.dk; hjorring@domstol.dk; holstebro@domstol.dk; horsens@domstol.dk; kolding@domstol.dk; lyngby@domstol.dk; nykobing@domstol.dk; naestved@domstol.dk; odense@domstol.dk; randers@domstol.dk; roskilde@domstol.dk; svendborg@domstol.dk; sonderborg@domstol.dk; viborg@domstol.dk; bornholm@domstol.dk; frederiksberg@domstol.dk; rigsadvokaten@ankl.dk; politi@politi.dk; JP-SKM; post@shret.dk; post@vestrelandsret.dk; post@oestrelandsret.dk
Emne: Høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger - (2016-7910-0008)

Se vedhæftede bilag.

Med venlig hilsen

JUSTITSMINISTERIET
IT og Service
Slotsholmsgade 10
1216 København K
Tlf.: 7226 8400
www.justitsministeriet.dk
jm@jm.dk

Vestre Landsret
Præsidenten

Justitsministeriet
IT og Service
Slotsholmsgade 10
1216 København K

Sendt pr. mail til databeskyttelseskontoret@jm.dk og kra@jm.dk

J.nr. 40A-VL-21-17
Den 15/03-2017

Justitsministeriet har ved mail af 1. marts 2017 (sagsnr. 2016-7910-0008) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger.

Efter det oplyste nedsættes der i Domstolsstyrelsen en arbejdsgruppe, der skal overveje det fremsendte udkast. Landsretten ønsker derfor ikke på nuværende tidspunkt at udtale sig om udkastet.

Med venlig hilsen

Helle Bertung

DATATILSYNET

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendt til: databeskyttelseskontoret@jm.dk
Kopi til: kra@jm.dk

15. marts 2017

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2017-111-0122
Dok.nr. 421581
Sagsbehandler
Sissel M Kristensen
Direkte 3319 3227

Vedrørende høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger, ministeriets j.nr. 2016-7910-0008

Ved e-mail af 1. marts 2017 har Justitsministeriet sendt ovenstående udkast i høring og anmodet om Datatilsynets bemærkninger hertil.

Datatilsynet har følgende bemærkninger til udkastet:

Ad § 1
Datatilsynet går ud fra, at der med formuleringen "automatisk databehandling" ikke er tilsigtet en indholdsmæssig ændring i forhold til begrebet "elektronisk databehandling", som fremgår af persondataloven.

Datatilsynet skal på den baggrund henstille, at formuleringen ændres, eller at det i bemærkningerne til lovforslaget understreges, at der ikke er tilsigtet en ændring i forhold til det eksisterende begreb.

I forhold til angivelsen af de myndigheder, hvis behandlinger af personoplysninger med de omhandlede formål skal være omfattet af loven, finder Datatilsynet, at det bør overvejes specifikt at nævne Hvidvasksekretariatet, eventuelt i bemærkningerne til lovforslaget.

Ad § 3
Datatilsynet har konstateret, at begrebet "pseudonymisering" – som er defineret i direktivets artikel 3, nr. 5 – ikke er medtaget i bestemmelsen.

Det er Datatilsynets erfaring, at det er en udbredt opfattelse, at pseudonymisering kan ligestilles med anonymisering. Dette kan i praksis medføre, at der foretages ulovlig behandling af personoplysninger.

Begrebet "personoplysninger" er defineret i persondataloven, men denne definition har i praksis ikke i fornødent omfang bidraget til en korrekt forståelse og adskillelse af begreberne "anonymisering" og "pseudonymisering".

Det er på den baggrund Datatilsynets opfattelse, at det vil være hensigtsmæssigt at medtage en definition af pseudonymisering i lovforslagets § 3, ligesom

det bør understreges i bemærkningerne til bestemmelsen, at der efter foretagelse af pseudonymisering fortsat vil være tale om personoplysninger.

Ad § 8
I forbindelse med inddelingen af registrerede i kategorier er det Datatilsynets opfattelse, at der kan være behov for at tage stilling til, hvordan de kompetente myndigheder skal behandle oplysninger om personer, som kan kategoriseres som både offer og sigtet/mistænkt i forbindelse med samme kriminelle handling. Tilsynet kan i den forbindelse til orientering henvise til en rapport, udarbejdet i 2015 af Den Fælles Kontrolmyndighed (JSB) for Europol, vedrørende ofre for menneskehandel.

Ad § 12
Datatilsynet er umiddelbart uforstående over for den foreslåede bestemmelse. Der er efter Datatilsynets opfattelse ikke belæg for at antage, at indberetning forudsættes at ske til tilsynsmyndigheden, og tilsynet finder ikke en sådan ordning hensigtsmæssig.

Det er Datatilsynets forståelse af direktivets artikel 48, at der i denne bestemmelse lægges op til en almindelig intern whistleblowerordning, som administreres af de kompetente myndigheder, herunder databeskyttelsesrådgiveren.

Ad § 17, stk. 3
Det er Datatilsynets umiddelbare opfattelse, at der i tilfælde, hvor der skal ske berigtigelse, jf. § 17, stk. 1, 1. pkt., ikke ses at være hjemmel i direktivet til at fastsætte bestemmelse om, at der i stedet for berigtigelse skal ske begrænsning. Datatilsynet stiller sig på den baggrund uforstående over for formuleringen af § 17, stk. 3.

Det fremgår af punkt 2.4.3.3. i de almindelige bemærkninger, at udøvelsen af retten til berigtigelse mv. i forhold til retsafgørelser skal ske efter retsplejelovens regler.

Datatilsynet skal i den forbindelse pege på, at der i praksis vil være en ikke ubetydelig del af straffesagerne, som *ikke* bliver underlagt domstolsprøvelse, f.eks. fordi sagen afgøres med et bødeforelæg, eller tiltale frafaldes. Den registrerede vil derfor ikke ad rettens vej få mulighed for at få prøvet/berigtiget oplysninger, som efter den pågældendes opfattelse er urigtige.

Ad § 18
Datatilsynet bemærker, at alene direktivets artikel 12, stk. 1, 1. pkt., ses at blive gennemført ved bestemmelsen.

Derimod ses lovforslaget ikke at indeholde bestemmelser til gennemførelse af direktivets artikel 12, stk. 1, 2. pkt., hvorefter oplysningerne skal gives på enhver hensigtsmæssig måde, herunder ved hjælp af elektroniske midler, samt § 12, stk. 1, 3. pkt., hvorefter den dataansvarlige som hovedregel skal give oplysningerne i samme form som anmodningen.

Ad § 20
Datatilsynet foreslår, at bestemmelsens stk. 1, 2. pkt., i overensstemmelse med direktivets artikel 19, stk. 2, formuleres således:

"Hvis det står i rimelig forhold til behandlingsaktiviteterne, skal disse foranstaltninger tillige omfatte passende databeskyttelsespolitikker".

Datatilsynet bemærker i øvrigt, at det i de almindelige bemærkninger til lovforslaget pkt. 2.5.3.1. og i bemærkningerne til § 20 er anført, at kravet i direktivets artikel 20 om databeskyttelse gennem design og standardindstillinger efter Justitsministeriets opfattelse ikke stiller krav om, at eksisterende systemer skal redesignes, men at kravene alene er relevante i forhold til udvikling og design af *fremtidige* systemer.

Datatilsynet skal hertil bemærke, at det i den forbindelse må være en forudsætning, at der ikke sker væsentlige ændringer i behandlingen af oplysninger i de eksisterende systemer.

Der henvises endvidere til det nedenfor anførte vedrørende lovforslagets § 26.

Ad § 22, stk. 1
Datatilsynet finder, at der i bemærkningerne til loven bør gives eksempler på, hvordan den dataansvarlige kan påse, at databehandleren træffer de i §§ 20 og 24 nævnte tekniske og organisatoriske sikkerhedsforanstaltninger. Sådanne foranstaltninger kunne være indhentelse af en uvildig revisionserklæring, hvor persondatasikkerheden er påset, fysisk besøg eller en procedure for et kontinuerligt tjek af databehandlerens persondatasikkerhedspolitikker.

Ad § 23
Det er Datatilsynets opfattelse, at der bør indsættes en bestemmelse om, at de i bestemmelsen omhandlende fortegnelser - både efter stk. 1 og stk. 2 - på anmodning stilles til rådighed for tilsynsmyndigheden, jf. herved også direktivets artikel 24, stk. 3.

Ad § 24
På baggrund af bemærkningerne til bestemmelsen må Datatilsynet forstå, at det ikke er hensigten, at direktivets krav om logning, jf. artikel 25, skal finde anvendelse fra lovens foreslåede ikrafttrædelsesdato den 1. maj 2017.

Det bemærkes i den forbindelse, at der ikke i udkastet ses at være fastsat bestemmelse om en udskudt ikrafttrædelsesdato for § 24. Tilsynet skal i den forbindelse gøre opmærksom på, at udkastets § 24, stk. 1, vil indebære et krav om logning med virkning fra den 1. maj 2017.

Ad § 26
Det fremgår af lovforslaget, at der alene skal ske høring af tilsynsmyndigheden inden behandling af personoplysninger i *nye registre*. Det er i den forbindelse angivet i bemærkningerne til lovforslaget, at ordningen kan sammenlignes med den eksisterende anmeldelsesordning.

Datatilsynet skal hertil bemærke, at det efter de gældende regler er *behandlingen* af personoplysninger, der udløser anmeldelsespligt, og ikke benyttelse af et nyt register/system. Der udløses endvidere fornyet anmeldelsespligt i tilfælde, hvor den dataansvarlige i forbindelse med et allerede etableret system/register, foretager en ny/ændret behandling af personoplysninger, der kan medføre en høj risiko for fysiske personers rettigheder.

Datatilsynet foreslår på den baggrund, at kravet om høring af tilsynsmyndigheden, i stedet knyttes til nye og væsentligt ændrede *behandlinger*, som medfører en (fornyet) høj risiko for fysiske personers rettigheder.

Tilsvarende betragtninger gør sig gældende for lovforslagets *§ 25.*

Ad § 28, stk. 5
Datatilsynet bemærker, at der efter tilsynets opfattelse bør fastsættes en nærmere angivet opbevaringsperiode for den dokumentation, som den dataansvarlig skal tilvejebringe efter bestemmelsen. Datatilsynet foreslår i den forbindelse, at opbevaringsperioden fastsættes til mindst 5 år fra det tidspunkt, hvor sikkerhedsbruddet er ophørt, eller fra det tidspunkt, hvor den dataansvarlige har kunnet dokumentere sikkerhedsbruddet, afhængig af hvilken dato der er senest.

Datatilsynet finder endvidere, at der bør indsættes en bestemmelse om, at den omhandlede dokumentation på anmodning skal stilles til rådighed for tilsynsmyndigheden, jf. herved også direktivets artikel 30, stk. 5, 2. pkt.

Ad § 40, stk. 2
Datatilsynet foreslår, at bestemmelsen erstattes med følgende ordlyd i overensstemmelse med direktivets artikel 46, stk. 2:

"Tilsynsmyndigheden letter indgivelsen af klager efter stk. 1, nr. 6".

Afslutningsvis bemærkes, at Datatilsynet forudsætter at blive hørt over eventuelle bekendtgørelser, der udstedes i medfør af loven, herunder eventuelle ændringer af gældende bekendtgørelser, der er udstedt med hjemmel i persondataloven.

Med venlig hilsen

Birgit Kleis
Kommitteret

Advokatrådet

ADVOKAT SAMFUNDET

Justitsministeriet
Slotsholmsgade 10
1216 København K

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF. 33 96 97 98

DATO: 15. marts 2017
SAGSNR.: 2017 - 761
ID NR.: 451214

databeskyttelseskontoret@jm.dk + kra@jm.dk

Høring - over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger

Ved e-mail af 1. marts 2017 har Justitsministeriet anmodet om Advokatrådets bemærkninger til ovennævnte forslag.

Høringsmaterialet er fremsendt med en frist på 14 dage til afgivelse af et svar.

Advokatrådet skal hertil bemærke, at en sådan frist – set i relation til forslagets omfang og kompleksitet – i realiteten udelukker en nærmere stillingtagen til de forslag, der er indeholdt i høringsmaterialet. Det må på den baggrund påregnes, at en række myndigheder og organisationer reelt ikke har mulighed for at udfylde den funktion som høringspart, som det lovforberedende arbejde normalt trækker på som led i kvalitetssikringen af ny regulering og som led i en almindelig, demokratisk proces.

Advokatrådet har på den baggrund ikke haft mulighed for at fremkomme med bemærkninger til høringssagen indenfor den fastsatte frist.

Med venlig hilsen

Torben Jensen

Østre Landsret
Præsidenten

Den 17 MAR. 2017
J.nr. 40A-ØL-20-17
Init: cr

Justitsministeriet
Lovafdelingen

Sendt pr. mail til databeskyttelseskontoret@jm.dk og kra@jm.dk

Justitsministeriet har ved brev af 1. marts 2017 (Sagsnr. 2016-7910-0008) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger (gennemførelse af direktiv om databeskyttelse på retshåndhævelsesområdet).

Efter det oplyste nedsættes der i Domstolsstyrelsen en arbejdsgruppe, der blandt andet skal overveje det fremsendte udkast. Henset hertil ønsker landsretten for nuværende ikke at udtale sig om udkastet.

Med venlig hilsen

Bent Carlsen

Ellen Busch Porsbo

KRIMINAL FORSORGEN

Koncernledelsessekretariatet

Direktoratet for Kriminalforsorgen

Sagsnr. 17-640-0025

Justitsministeriet
Databeskyttelseskontoret

15. marts 2017

Høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger

Justitsministeriet har ved skrivelse af 1. marts 2017, j.nr. 2016-7910-0008, anmodet om eventuelle bemærkninger til udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger.

I den anledning kan direktoratet oplyse, at man ikke har bemærkninger til lovudkastet.

Med venlig hilsen

Vibeke Greve
Enhedsleder, Jura

[redacted]
Strandgade 100 | 1401 København K | Tlf. 7255 5555
dfk@kriminalforsorgen.dk | www.kriminalforsorgen.dk

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendt per email til **databeskyttelseskontoret@jm.dk**
med kopi til **kra@jm.dk**

IT-Politisk Forening
c/o Jesper Lund
Carl Bernhards Vej 15, 2.tv
1817 Frederiksberg C

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 15. marts 2017

Høringssvar vedr. lovforslag om retshåndhævende myndigheders behandling af personoplysninger

På grund af den relativt korte tidsfrist og lovforslagets omfang har IT-Politisk Forening i dette høringssvar fokuseret på den registreredes rettigheder, databeskyttelse gennem design og standardindstillinger, samt enkelte andre bestemmelser i lovforslaget, som efter vores vurdering har stor betydning for borgernes grundlæggende ret til privatliv og persondatabeskyttelse.

Den registreredes rettigheder

For politiets behandling af personoplysninger på det strafferetlige område har persondatalovens § 2, stk. 4 en fuldstændig undtagelse for oplysningspligten over for den registrerede (kapitel 8), indsigelse mod og berigtigelse af forkerte oplysninger (§§ 35-37), samt automatiske afgørelser og profilering (§ 39). Retten til indsigt hos politiet er på en række områder fuldstændigt afskåret via persondatalovens § 32, stk. 5. Det gælder også for politiets behandling af personoplysninger i forbindelse med automatisk nummerpladegenkendelse (ANPG), selvom en betydelig del af registreringen i ANPG-systemet ikke har nogen relation til efterforskningen af konkrete igangværende straffesager.

I Politiets Efterforskningsstøtte Database (PED) er retten til indsigt ligeledes fuldstændigt afskåret via persondatalovens § 32, stk. 5. Personoplysninger i

persondelen skal jf. PED-bekendtgørelsens § 10, stk. 1 først slettes 10 år efter at der senest er indlagt oplysninger om en person. Borgerne kan derfor være opført i PED i lang tid (10 år) efter at en mistanke mod dem i forbindelse med en politimæssig efterforskning er fuldstændigt afklaret, og borgerne vil heller ikke i den situation (hvor der ikke er nogen efterforskning) kunne få indsigt i personoplysninger om dem.

I Det Centrale Kriminalregister (Kriminalregisteret) er retten til indsigt også kraftigt begrænset, idet borgerne alene kan få indsigt i de oplysninger som fremgår af straffeattesten, dvs. oplysninger fra Kriminalregisterets afgørelsesdel, som borgerne vel må formodes at være bekendt med i forvejen. Der er ingen indsigt i oplysninger i efterforskningsdelen (bilag 2 i bekendtgørelsen om Kriminalregisteret), selvom der her kan registreres en lang række oplysninger om borgerne, herunder betegnelser (aktualitetsmarkeringer) som "uromager", "farlig" eller "narkobruger", som kan have væsentlig betydning for borgernes kontakt med politiet i det offentlige rum og deres rettigheder og frihedsrettigheder, ligesom der kan være tale om personoplysninger som borgerne selv mener er ukorrekte. Politiet kan også registrere visse helbredsoplysninger i Kriminalregisteret under aktualitetsmarkeringerne. De fleste aktualitetsmarkeringer slettes først efter 20 år.

Hvis der er tale om personoplysninger som er modtaget fra et andet EU-land i henhold til Rådets afgørelse 2008/977/RIA (rammeafgørelsen) vil der under gældende dansk ret (rammeafgørelsesbekendtgørelsen, BEK nr 1287 af 25/11/2010) være ret til indsigt, indsigelse og berigtigelse, altså en bedre retsstilling end efter persondatalovens almindelige regler på det strafferetlige område.

Retshåndhævelsesdirektet må generelt indebære en betydelig styrkelse af den registreredes rettigheder, især i forhold til politiets rent nationale behandling af personoplysninger, som ikke er omfattet af EU-retlige forpligtelser i dag, men også i forhold til rammeafgørelsesbekendtgørelsen.

Således er der efter retshåndhævelsesdirektivet som udgangspunkt en oplysningspligt over for den registrerede,

ret til indsigt, samt ret til indsigelse og berigtigelse. Denne ret er selvfølgelig ikke absolut, idet den kan begrænses ved lov, ligesom det er tilfældet i dag efter persondatalovens § 30, stk. 2 i forhold til indsigtsretten (og oplysningspligten, hvor der dog er en mere generel undtagelse på det strafferetlige område).

Retshåndhævelsesdirektivets muligheder for at begrænse indsigtsretten fremgår af artikel 15, stk. 1, som i lovforslaget er gennemført ved § 16 og § 14, stk. 1. Selv om de overordnede begrundelser minder meget om persondatalovens § 30, stk. 2, er det IT-Politisk Forenings klare opfattelse, at betingelserne for at begrænse indsigtsretten er mere restriktive i retshåndhævelsesdirektivet. Det skyldes især det nye krav om at indskrænkningen skal udgøre en "nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund under behørigt hensyn til den berørte fysiske persons grundlæggende rettigheder og legitime interesser". Af retshåndhævelsesdirektivets betragtning 44 fremgår det desuden, at den dataansvarlige gennem en konkret og individuel undersøgelse af de enkelte tilfælde skal vurdere, om indsigtsretten helt eller delvist bør begrænses.

Det er meget svært at vurdere, om lovforslaget reelt afspejler den styrkelse af de registreredes rettigheder, som gennemførelse af retshåndhævelsesdirektivet må antages at medføre. Det skyldes at lovforslaget i § 14, stk. 1 alene nævner de overordnede begrundelser for at begrænse de registreredes rettigheder fra direktivet (direktivets artikel 15, stk. 1), og overlader det til Justitsministeren at fastsætte nærmere regler om disse begrænsninger i bekendtgørelser. Justitsministeren får efter § 16, stk. 4 også mulighed for at fastsætte regler om, at begæringer om indsigt i almindelighed må nægtes, ligesom den nuværende § 32, stk. 5 i persondataloven. Det sidste synes umiddelbart at være i strid med kravet i betragtning 44 om en konkret og individuel undersøgelse af de enkelte anmodninger om indsigt.

IT-Politisk Forening har forståelse for, at begrænsningerne af retten til indsigt (og de øvrige rettigheder for den registrerede) fastsættes i en bekendtgørelse. Men der er efter vores opfattelse behov for en gennemgribende re-vurdering af de eksisterende begrænsninger af indsigtsretten, som er næsten alt-omfattende for politiets

behandling af personoplysninger på det strafferetlige område. Det gælder især ANPG-registeret, hvor registreringerne i mange tilfælde er helt uden tilknytning til konkrete efterforskninger, som der selvfølgelig er et legitimt behov for at beskytte. Men der er også behov for en revurdering i forhold til bekendtgørelserne om PED og Kriminalregisteret, hvor personoplysninger kan behandles i meget lang tid (10-20 år) efter at en politimæssig efterforskning er afsluttet, og stadig uden at der er nogen ret til indsigt.

Det er vanskeligt at se, at den nye ret til indsigelse mod behandling af ukorrekte personoplysninger og berigtigelse af disse (lovforslagets § 17), kan have et reelt indhold, hvis retten til indsigt er afskåret på samme generelle måde som i dag. Uden kendskab til indholdet af de personoplysninger, som politiet behandler om borgerne, er det generelt svært at gøre brug af en formel ret til at gøre indsigelse mod ukorrekte oplysninger og få disse oplysninger berigtiget.

Lovforslagets § 55, stk. 2 har en ikrafttrædelsesbestemmelse om, at regler udstedt i medfør af bl.a. § 32, stk. 5 og § 72 i persondataloven fortsat finder anvendelse, medmindre det vil være i strid med denne lov (lov om retshåndhævende myndigheders behandling af personoplysninger).

Hertil skal IT-Politisk Forening bemærke, at retshåndhævelsesdirektivets betragtning 33 stiller krav til lovgrundlaget, især dets tilgængelighed og forudsigelighed (dette uddybes i vores bemærkninger nedenfor i afsnittet om begrebet "lov"). Det kan på den baggrund ikke være overladt til borgerne selv at vurdere hvilke dele af eksempelvis ANPG-bekendtgørelsen, PED-bekendtgørelsen eller bekendtgørelsen om Kriminalregisteret, som fortsat finder anvendelse, fordi de pågældende bestemmelser ikke strider mod retshåndhævelsesdirektivet. Specielt i forhold til bestemmelser om begrænsninger af de registreredes rettigheder, for eksempel retten til indsigt, er denne usikkerhed om retstilstanden meget problematisk.

Justitsministeriet må hurtigst muligt revidere de eksisterende bekendtgørelser udstedt efter persondataloven, så de ikke strider mod den nye lov om retshåndhævende myndigheders behandling af

personoplysninger.

Databeskyttelse gennem design og gennem standardindstillinger

Retshåndhævelsesdirektivet indfører, ligesom databeskyttelsesforordningen 2016/679/EU, bestemmelser om databeskyttelse gennem design og gennem standardindstillinger for blandt andet at understøtte de generelle krav om formålsbegrænsning, dataminimering og behandlingssikkerhed, som allerede fremgår af den gældende persondatalov (baseret på persondatadirektivet 95/46/EF). Et eksempel på databeskyttelse gennem design kunne være pseudonymisering, som i øvrigt omtales i udkastet til lovforslag af 10. februar 2017 vedrørende politiets anvendelse af databaserede analyseredskaber (intelligence-led policing).

Retshåndhævelsesdirektivets artikel 20 om databeskyttelse gennem design og gennem standardindstillinger gennemføres med § 20, stk. 2 i lovforslaget. Ifølge de almindelige bemærkninger pkt. 2.5.3.1 mener Justitsministeriet imidlertid ikke, at kravet om databeskyttelse gennem design og gennem standardindstillinger omfatter eksisterende systemer til behandling af personoplysninger. Derfor fastsættes det i § 53, stk. 2, at § 20, stk. 2 kun gælder for automatiske databehandlingssystemer, der idriftsættes den 1. maj 2017 eller senere.

IT-Politisk Forening undrer sig over denne fortolkning af artikel 20 i retshåndhævelsesdirektivet. Efter vores læsning af direktivet er eksisterende systemer omfattet af bestemmelserne om databeskyttelse gennem design og gennem standardindstillinger. Nogle af de hensyn, som er nævnt i artikel 20 stk. 1, især implementeringsomkostningerne, vil givetvis afhænge af, om der er tale om et nyt system eller et eksisterende system, men det er ikke det samme som at eksisterende systemer helt kan undtages fra artikel 20.

IT-Politisk Forenings vurdering er baseret på de følgende tre argumenter. For det **første** henviser direktivets artikel 20, stk. 1 både til "tidspunktet for fastlæggelse af midlerne til behandling" og til "tidspunktet for selve behandlingen",

og den dataansvarlige skal tage hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne, og de risici som behandlingen skaber for fysiske personers rettigheder og frihedsrettigheder. At tidspunktet for behandlingen nævnes understøtter, at eksisterende systemer er omfattet af kravene. I betragtning 53 indgår databeskyttelse gennem design og gennem standardindstillinger som et direkte element i påvisningen af, at den dataansvarlige overholder direktivet. For det **andet** er der i artikel 20 ikke som i artikel 28 en direkte henvisning til et "nyt register" eller "nye teknologier" som i artikel 27. For det **tredje**, må gennemførelses-bestemmelserne i direktivets artikel 63 opfattes som en udtømmende liste af tilfælde, hvor retshåndhævelses-direktivets krav kan fraviges midlertidigt i forhold til eksisterende systemer. Artikel 63, stk. 2 og 3 tillader at logningskravene i direktivets artikel 25, stk. 1 (der er udvidet i forhold til den nuværende sikkerhedsbekendtgørelse) i ekstraordinære tilfælde kan udskydes til 2023 eller endog til 2026 under ekstraordinære omstændigheder med alvorlige vanskeligheder. Men der er ikke i artikel 63 nogen tilsvarende henvisning til artikel 20. Skæringsdatoen i artikel 63 er i øvrigt 6. maj 2016 (direktivets ikrafttrædelsesdato) og ikke datoen for medlemsstaternes gennemførelse af direktivet (dvs. 1. maj 2017 for Danmarks vedkommende).

Den tidsmæssigt ubegrænsede undtagelse fra kravene om databeskyttelse gennem design og gennem standardindstillinger, som Justitsministeriet foreslår i lovforslagets § 53, stk. 2 for eksisterende databehandlingssystemer, vil i øvrigt volde betydelige praktiske fortolkningsproblemer. Hvornår er et eksisterende system til automatisk databehandling modificeret så meget, at der er tale om et nyt system som er idriftsat efter den 1. maj 2017? Formentlig sker der løbende små eller store justeringer af eksempelvis Kriminalregisterets systemer, og det kan næppe være Justitsministeriets hensigt, at der aldrig nogensinde skal være krav om databeskyttelse gennem design i Kriminalregisteret.

Forskellige kategorier af registrerede

Efter lovforslagets § 8 skal den dataansvarlige så vidt muligt sondre mellem forskellige kategorier af registrerede (mistænkte, dømte, ofre og andre parter).

I den forbindelse vil IT-Politisk Forening påpege, at politiet i ANPG-systemet og formentlig også i fremtidige systemer til intelligence-led policing (herunder POL-INTEL) inden for strafferetsplejen behandler personoplysninger om borgere, som ikke er mistænkte for strafbare handlinger. Når politiet indsamler oplysninger om ikke-mistænkte personer til eksempelvis intelligence-led policing formål, bør den nye bestemmelse i lovforslagets § 8 som minimum føre til, at der i forhold til kravene i den eksisterende lovgivning (persondataloven) fastsættes højere krav til beskyttelsen af denne kategori af registrerede.

I ANPG-bekendtgørelsen er der efter IT-Politisk Forenings opfattelse behov for bestemmelser, som konkret og reelt beskytter borgere mod at de kan blive mistænkt for en strafbar handling på grundlag af dataanalyse af deres kørselsmønstre og kørselsadfærd (profilering). Den eksisterende § 7 i ANPG-bekendtgørelsen giver ikke borgerne denne beskyttelse mod profilering, specielt ikke når der er tale om kriminalitet som er omfattet af en målrettet politimæssig indsats, idet en målrettet politimæssig indsats samtidig giver mulighed for en væsentlig udvidelse af registreringerne i ANPG-systemet (registrering af no-hits efter ANPG-bekendtgørelsens § 6, stk. 1). Det er netop i den situation, hvor indsamlingen af oplysninger om ikke-mistænkte borgere kraftigt forøges, at der er behov for en yderligere beskyttelse af denne kategori af registrerede.

Begrebet "lov"

Retshåndhævelsesdirektet giver medlemsstaterne muligheder for at fastsætte en række bestemmelser ved lov, herunder ikke mindst begrænsninger af den registreredes rettigheder. Efter direktivets betragtning 33 skal "lov" forstås bredt i den forstand, at det ikke behøver at være love vedtaget af et parlament, men der stilles til gengæld en række krav til lovgrundlaget, uanset om det eksempelvis er en lov vedtaget af Folketinget eller en

bekendtgørelse udstedt Justitsministeren. Det fremgår konkret af betragtning 33, at lovgrundlaget skal være klart, præcist og forudsigeligt i overensstemmelse med kravene i retspraksis fra EU-Domstolen og den Europæiske Menneskerettighedsdomstol:

> *En sådan national ret i medlemsstaterne, et sådant retsgrundlag eller en sådan lovgivningsmæssig foranstaltning bør imidlertid være klar(t) og præcis(t), og anvendelse heraf bør være forudsigelig for de personer, der er omfattet af dets/dens anvendelsesområde, jf. retspraksis fra Domstolen og Den Europæiske Menneskerettighedsdomstol.*

Betragtning 33 nævnes ikke i lovforslagets bemærkninger, hvilket selvfølgelig ikke er nødvendigt, blot love og bekendtgørelser lever op til kravene i betragtning 33. Men af lovforslagets pkt. 2.3.3.1 (side 59) fremgår det omvendt, at

> *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.*

Hertil skal IT-Politisk Forening bemærke, at der må være grænser for hvor "generel" en lovhjemmel kan være i forhold til kravene i direktivets betragtning 33.

Undtagelser for efterretningstjenesterne

Lovforslagets § 1, stk. 2 har en generel undtagelse for Politiets Efterretningstjeneste (PET) og Forsvarets Efterretningstjeneste (FE). Det begrundes i bemærkningerne med at retshåndhævelsesdirektivet ikke finder anvendelse på aktiviteter, som falder uden for EU-retten, for eksempel national sikkerhed.

IT-Politisk Forening vil anbefale, at undtagelsen for national sikkerhed formuleres på samme måde som i retshåndhævelsesdirektivets artikel 2, stk. 3, litra a, dvs. som en undtagelse vedrørende udøvelsen af aktiviteter, der falder uden for EU-retten, i stedet for en generel

undtagelse vedrørende PET og FE som sådan.

PET har tidligere beskæftiget sig med andre opgaver end straffelovens kapitel 12 og 13, og der vil givetvis også i fremtiden være andre situationer, hvor især PET men måske også FE udfører opgaver inden for EU-retten og retshåndhævelsesdirektivets anvendelsesområde. Ifølge Forsvarsministeriets vurdering i lovforslag L 146 af 24. februar 2017 er FEs modtagelse af PNR-oplysninger fra SKAT eksempelvis omfattet af EU-retten.

Hvis der mellem EU-landene skal udveksles oplysninger om personer, som er mistænkt for terrorisme, vil det generelt være hensigtsmæssigt, at der gælder passende databeskyttelsesregler for de overførte personoplysninger. Nogle EU-lande vil måske være tilbageholdende med at overføre personoplysninger om konkrete terrormistænkte personer til Danmark, hvis retshåndhævelsesdirektivets databeskyttelsesregler reelt ikke gælder, fordi personoplysningerne havner hos PET.

Terrorisme er meget ofte grænseoverskridende kriminalitet, og der er givetvis behov for et tættere samarbejde mellem EU-landene på dette område, herunder ikke mindst informationsudveksling om konkrete mistænkte personer. Det er meget bedre end masseovervågning af hele befolkningen. Hvis alle EU-lande fastholder retten til at udvande persondatabeskyttelsen i retshåndhævelsesdirektivet med henvisning til national sikkerhed, kan det meget vel få negative konsekvenser for informationsudvekslingen mellem EU-landene, og ultimativt for effektiviteten af terrorbekæmpelsen i Europa.

Særlige bestemmelser for CPR-nummeret

Ifølge bemærkningerne pkt. 2.3.3.5 er der efter Justitsministeriets opfattelse ikke behov for at fastsætte særlige bestemmelser om behandling af personnummeret svarende til persondatalovens § 11. Behandling af personnummeret sikrer en entydig identifikation af borgeren i retshåndhævende myndigheders systemer, og persondatalovens § 11 begrænser alene private dataansvarliges behandling af personnummeret.

Hvis der sker et brud på datasikkerheden som omfatter

personnummeret, kan dette give alvorlige problemer for borgerne, selv i den situation hvor bruddet alene omfatter personnummeret og eventuelt borgerens navn. Det skyldes, at personnummeret anvendes generelt i den offentlige forvaltning og nogle private virksomheder, og at personnummeret dermed kan bidrage til at sammenkæde oplysninger om borgeren fra forskellige kilder, herunder fra brud på datasikkerheden hos andre dataansvarlige, til en samlet profil af borgeren. Et brud på datasikkerheden som omfatter personnummeret vil derfor efter IT-Politisk Forenings opfattelse så godt som altid indebære en høj risiko for fysiske personer rettigheder i forhold til lovforslagets § 29, stk. 1 (og dermed krav om underretning af de registrerede ved brud på datasikkerheden).

IT-Politisk Forening vil opfordre til at denne sammenhæng mellem personnummeret og "høj risiko" i forbindelse med brud på datasikkerheden nævnes i bemærkningerne. Det vil også give retshåndhævende myndigheder et yderligere incitament til at gennemføre databeskyttelse gennem design, idet underretning af den registrerede ved brud på datasikkerheden kan udelades, hvis den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, for eksempel pseudonymisering og kryptering, jf. retshåndhævelsesdirektivets artikel 31, stk. 3, litra a. Den økonomiske risiko for databehandlere vil også blive mindre.

Særlige kategorier af personoplysninger

Ved behandling af særlige kategorier af personoplysninger (følsomme personoplysninger) er der i lovforslagets § 10 et krav om streng nødvendighed for at behandle disse personoplysninger, hvilket er et skærpet krav i forhold til behandling af almindelige personoplysninger, som blot skal være nødvendigt.

I bemærkningernes pkt. 2.3.3.6 anfører Justitsministeriet, at det i praksis formentlig ikke vil være muligt at angive nogen væsentlig forskel på kriterierne "nødvendigt" og "strengt nødvendigt". Det begrundes med at oplysninger om eksempelvis politisk overbevisning kun vil blive behandlet i forbindelse med et politisk motiveret mord.

IT-Politisk Forening vil dog samtidig påpege, at der i Kriminalregisteret kan behandles visse helbredsoplysninger om borgerne, og at disse oplysninger kan opbevares i meget lang tid. Kravet om streng nødvendighed for at behandle helbredsoplysninger og andre følsomme personoplysninger er en skærpelse i forhold til persondatalovens § 7, stk. 6, som alene kræver at behandlingen skal være nødvendig. Det bør give anledning til en fornyet vurdering af behandlingsreglerne for helbredsoplysninger i eksempelvis Kriminalregisteret.

Udover det skærpede behandlingskrav om streng nødvendighed udvider retshåndhævelsesdirektivet definitionen af særlige kategorier af personoplysninger (følsomme personoplysninger) i forhold til persondataloven. Biometriske data med det formål entydigt at identificere en person er i dag almindelige personoplysninger, men vil fremover falde ind under særlige kategorier af personoplysninger. Det har blandt andet betydning for fingeraftryk og automatisk ansigtsgenkendelse. IT-Politisk Forening er ikke bekendt med at dansk politi anvender automatisk ansigtsgenkendelse i forbindelse med videoovervågning, men det er ikke utænkeligt at Rigspolitiet og Justitsministeriet vil overveje automatisk ansigtsgenkendelse i fremtiden (eller allerede har gjort det). Når behandlingen af personoplysninger er knyttet til en generel overvågning i det offentlige rum som videovervågning, er forskellen mellem nødvendig og streng nødvendig formentlig større end eksemplerne i bemærkningernes pkt. 2.3.3.6.

IT-Politisk Forening vil også anbefale, at politiets behandlingsregler for fingeraftryk og DNA-profiler generelt genovervejes i lyset af at disse personoplysninger nu falder ind under særlige kategorier af personoplysninger, hvilket i en eventuel interesseafvejning mellem politiets og den registreredes interesser alt andet lige må føre til et øget hensyn til den registreredes rettigheder og frihedsrettigheder.

Fortegnelser over behandlingsaktiviteter

Retshåndhævelsesdirektivet indfører et nyt krav om fortegnelser over behandlingsaktiviteter. Ifølge

lovforslagets bemærkninger svarer kravene til indholdet af disse fortegnelser til de eksisterende krav til indholdet af anmeldelser til Datatilsynet. Anvendelsesområdet udvides dog til alle behandlingsaktiviteter (jf. lovforslagets bemærkninger pkt. 2.5.3.4), mens der i dag kun er krav om anmeldelse på nogle områder, og databehandlere skal fremover også udarbejde fortegnelser. Efter anmodning skal den dataansvarlige og databehandleren stille fortegnelserne til rådighed for tilsynsmyndigheden (Datatilsynet eller Domstolsstyrelsen).

Anmeldelserne til Datatilsynet er i dag offentligt tilgængelige på hjemmesiden https://anmeld.datatilsynet.dk. Så vidt IT-Politisk Forening kan vurdere er dette ikke et krav i persondataloven, men anmeldelserne ville formentlig være omfattet af en anmodning aktindsigt efter offentlighedsloven hos Datatilsynet.

IT-Politisk Forening vil opfordre til, at fortegnelserne for de dataansvarliges behandlingsaktiviteter bliver gjort offentligt tilgængelige på samme måde som anmeldelserne er det i dag. Det kan enten ske på den dataansvarliges hjemmeside eller på Datatilsynets hjemmeside.

Offentliggørelsen af de nuværende anmeldelser er et nyttigt arbejdsredskab for organisationer som IT-Politisk Forening, der arbejder med privatliv og persondatabeskyttelse, og offentliggørelse af fortegnelserne kan kun bidrage til at styrke borgernes tillid til den offentlige sektors, herunder retshåndhævende myndigheders, behandling af personoplysninger. Hvis fortegnelserne indholdsmæssigt svarer til de nuværende anmeldelser, bør der ikke være noget problem med at offentliggøre dem (eksempelvis fortrolighedshensyn). Offentliggørelse vil samtidig spare tid for de retshåndhævende myndigheder i forhold til behandling af anmodninger om aktindsigt i fortegnelserne efter offentlighedsloven.

Kenny Rasmussen

Fra: Lise Krüger Andersen [LiseKruegerAndersen@Shret.dk]
Sendt: 17. marts 2017 14:15
Til: #951dep-Databeskyttelseskontoret; Kenny Rasmussen
Emne: SV: Høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger - (2016-7910-0008)

Lovforslaget giver ikke Sø- og Handelsretten anledning til bemærkninger.

Med venlig hilsen

Lise Krüger Andersen
Juridisk chef
Direkte: + 45 99 68 47 21
LiseKruegerAndersen@Shret.dk

Sø- og Handelsretten
Amaliegade 35, 2. sal
1256 København K.
Tlf.: 99 68 46 20
www.shret.dk

Fra: 'post@shret.dk'
Sendt: 2. marts 2017 09:22
Til: Lise Krüger Andersen
Emne: VS: Høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger - (2016-7910-0008)

Fra: Justitsministeriet [mailto:jm@jm.dk]
Sendt: 1. marts 2017 16:10
Til: samfund@advokatsamfundet.dk; mail@danskeadvokater.dk; dt@datatilsynet.dk; Mikael Sjöberg <MikaelSjoeberg@OestreLandsret.dk>; $Direktoratet for Kriminalforsorgen <dfk@kriminalforsorgen.dk>; hoeringer@dommerfm.dk; 'Domstolsstyrelsen' <post@domstolsstyrelsen.dk>; lsc@ankl.dk; info@humanrights.dk; 'Københavns Byret' <kobenhavn@domstol.dk>; pt@strafferetsadvokaten.dk; mail@politiforbundet.dk; 'Retten i Aalborg' <aalborg@domstol.dk>; 'Retten i Aarhus' <aarhus@domstol.dk>; 'Retten i Esbjerg' <esbjerg@domstol.dk>; 'Retten i Glostrup' <glostrup@domstol.dk>; 'Retten i Helsingør' <helsingor@domstol.dk>; 'Retten i Herning' <herning@domstol.dk>; 'Retten i Hillerød' <hillerod@domstol.dk>; 'Retten i Hjørring' <hjorring@domstol.dk>; 'Retten i Holstebro' <holstebro@domstol.dk>; 'Retten i Horsens' <horsens@domstol.dk>; 'Retten i Kolding' <kolding@domstol.dk>; 'Retten i Lyngby' <lyngby@domstol.dk>; 'Retten i Nykøbing' <nykobing@domstol.dk>; 'Retten i Næstved' <naestved@domstol.dk>; 'Retten i Odense' <Odense@domstol.dk>; 'Retten i Randers' <randers@domstol.dk>; 'Retten i Roskilde' <roskilde@domstol.dk>; 'Retten i Svendborg' <svendborg@domstol.dk>; 'Retten i Sønderborg' <sonderborg@domstol.dk>; 'Retten i Viborg' <viborg@domstol.dk>; 'Retten på Bornholm' <bornholm@domstol.dk>; 'Retten på Frederiksberg' <frederiksberg@domstol.dk>; rigsadvokaten@ankl.dk; politi@politi.dk; skm@skm.dk; 'post@shret.dk' <Post@Shret.dk>; 'Post@VestreLandsret.dk' <Post@VestreLandsret.dk>; 'Post@OestreLandsret.dk' <Post@OestreLandsret.dk>
Emne: Høring over udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger - (2016-7910-0008)

Se vedhæftede bilag.

Med venlig hilsen

JUSTITSMINISTERIET
IT og Service
Slotsholmsgade 10
1216 København K
Tlf.: 7226 8400
www.justitsministeriet.dk
jm@jm.dk

INSTITUT FOR
MENNESKE
RETTIGHEDER

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
DIREKTE 32698869
MOBIL 32698869
HSC@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 17/00538-2

15. MARTS 2017

Justitsministeriet
Slotsholmsgade 10
1216 København K
Danmark

Databeskyttelseskontoret@jm.dk
Kopi til kra@jm.dk

FORSLAG TIL LOV OM RETSHÅNDHÆVENDE MYNDIGHEDERS BEHANDLING AF PERSONOPLYSNINGER

Justitsministeriet har ved e-mail af 1. marts 2017 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til udkast til forslag til lov om retshåndhævende myndigheders behandling af personoplysninger (gennemførelse af direktiv om databeskyttelse på retshåndhævelsesområdet).

Folketinget meddelte ved beslutning af 25. oktober 2016 sit samtykke til, at regeringen tilslutter sig Europa-Parlamentets og Rådets direktiv (EU) 2016/680 om databeskyttelse på retshåndhævelsesområdet (herefter retshåndhævelsesdirektivet). Denne beslutning er meddelt Rådet den 26. oktober 2016. Retshåndhævelsesdirektivet er ikke til hinder for, at medlemsstaterne fastsætter højere standarder for beskyttelse af den registreredes rettigheder.

Det er en forudsætning for, at der kan indgås en samarbejdsaftale mellem Danmark og Europol med virkning fra den 1. maj 2017, at retshåndhævelsesdirektivet er gennemført inden denne dato.

Instituttet har følgende bemærkninger:

1. Begrænsning af den registreredes rettigheder

Reglerne i retshåndhævelsesdirektivet medfører, at den registreredes rettigheder bliver udvidet ganske betydeligt, da persondataloven ikke finder anvendelse på behandlinger, der foretages af politi, anklagemyndighed og domstole inden for det strafferetlige område.

Udkastets kapitel 4 vedrører blandt andet de oplysninger, som ifølge direktivet skal stilles til rådighed for eller gives til den registrerede, jf. herved udkastets § 13, og den registreredes indsigtsret efter udkastets § 15.

Ifølge retshåndhævelsesdirektivets artikel 13, stk. 3 og artikel 15, stk. 1, kan den registreredes indsigtsrettigheder begrænses, f.eks. for at beskytte statens sikkerhed, for at undgå at skade efterforskning eller retsforfølgelse af strafbare handlinger og for at beskytte andres rettigheder og frihedsrettigheder.

Lovudkastets § 14, stk. 1, nr. 5) og § 16, stk. 1, jf. § 14, stk. 1, bestemmer imidlertid, at den registreredes rettigheder - ud over de i direktivet angivne undtagelsessituationer - tillige kan indskrænkes, hvis den registrerede interesse i at få kendskab til oplysningerne findes at burde vige for at beskytte *den registreredes* rettigheder. En sådan begrænsning i den registreredes adgang til indsigt mv. fremgår ikke af direktivet. Databeskyttelsesforordningen (EU/2016/679) indeholder heller ikke denne mulighed for at begrænse den registreredes indsigt.

Persondataloven indeholder en adgang til at begrænse den registreredes indsigtsret efter § 30, stk. 1, 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. Denne begrænsning er blandt andet anvendt i sociale og familieretlige sager vedrørende børn og unges meget personlige forhold.

Det fremgår af lovudkastets almindelige bemærkninger side 76, at det efter Justitsministeriets opfattelse vil være hensigtsmæssigt, hvis det også fremover er muligt at begrænse indsigtsretten af hensyn til den registrerede selv. Denne begrænsning kan ifølge ministeriet navnlig 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 er instituttets opfattelse, 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 direktivets ordlyd, jf. herved også at databeskyttelsesforordningens artikel 15, stk. 4, indeholder en tilsvarende begrænsning.

- Instituttet anbefaler, at den registreredes indsigtsret fastlægges i overensstemmelse med retshåndhævelsesdirektivets ordlyd, artiklerne 13 og 15, således at indsigtsretten alene kan begrænses for at beskytte 'andres rettigheder og frihedsrettigheder'.

2. Erstatningsansvar for ulovlig behandling mv.

Retshåndhævelsesdirektivets artikel 56 bestemmer, at medlemsstaterne fastsætter regler om, at enhver person, som har lidt materiel eller immateriel skade som følge af en ulovlig

behandlingsaktivitet mv., har ret til erstatning for den forvoldte skade. Direktivet tager ikke stilling til, om det skal være et præsumptionsansvar (culpa med omvendt bevisbyrde) eller et almindeligt culpaansvar.

Den nugældende persondatalovs § 69 fastslår, at der gælder et skærpet ansvarsgrundlag i form af et præsumptionsansvar, således at den dataansvarlige skal bevise, at hverken den pågældende selv eller nogen, for hvis fejl den dataansvarlige i givet fald er ansvarlig for, har handlet culpøst.

Ifølge databeskyttelsesforordningens artikel 82 er en dataansvarlig eller en databehandler fritaget for erstatningsansvar, hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden i lighed med det præsumptionsansvar, der gælder i medfør af persondataloven.

Det foreslås i udkastets § 49, at det nugældende præsumptionsansvar ændres til et culpaansvar, således at skadevolderen skal have handlet culpøst og have forvoldt skaden ved forsætlig eller uagtsom adfærd. Ændringen begrundes med, at 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, side 117f.

Justitsministeriet henviser endvidere til de registreredes mulighed for at godtgøre, at der foreligger et erstatningsansvar, skal 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.

Det er instituttets opfattelse, at der ikke foreligger særlige grunde til at ændre på den gældende retstilstand, hvorefter der i disse sager gælder et skærpet ansvarsgrundlag, også selvom retshåndhævelsesdirektivet ikke indeholder krav om et sådant. Et præsumptionsansvar i disse sager vil også være i overensstemmelse med databeskyttelsesforordningens artikel 82.

- Instituttet anbefaler, at persondatalovens nuværende præsumptionsansvar videreføres i lov om retshåndhævende myndigheders behandling af personoplysninger.

Der henvises afslutningsvist til instituttets høringssvar af 21. september 2016, hvori instituttet blandt andet anførte, at direktivet ikke indeholder en beskyttelse af "semi-følsomme" personoplysninger, men at adgangen til at fastsætte højere nationale standarder vil kunne benyttes til at yde disse oplysninger en særlig beskyttelse. Denne adgang til en udvidet beskyttelse af disse oplysninger ses ikke udnyttet i det foreliggende lovudkast.

Under hensyn til den korte høringsfrist, har instituttet alene haft mulighed for at fremsætte sine bemærkninger på baggrund af en mere overordnet tilgang til lovudkastet med bilag.

Der henvises til ministeriets sagsnummer 2016-7910-0008.

Med venlig hilsen

Christoffer Badse
MONITORERINGSCHEF