.ıll 4G

Databeskyttelseskontoret
Att: Kontorchef Jakob Lundsager

København den 21. august 2017

Høring over udkast til forslag til databeskyttelsesloven
Hi3G har den 7. juli 2017 modtaget udkast til forslag til databeskyttelsesloven, hvortil Hi3G har følgende bemærkninger:

Behandling af personoplysninger i forbindelse med ansættelsesforhold § 12.
I lovforslagets § 12, stk. 3 foreslås det, at samtykke kan anvendes som behandlingsgrundlag ved personaleadministration. Dette er et kontroversielt forslag, idet artikel 29-gruppen har udtalt, at et sådant samtykke i ansættelsesforhold ikke opfattes som frivilligt. Samtykke i et ansættelsesforhold vil alene skulle anvendes i situationer, hvor medarbejdere reelt har mulighed for at kunne trække samtykket tilbage, og der må således ikke være tvivl om, at det givne samtykke er frivilligt. Artikel 29-gruppen har fastslået, at medarbejdere i et ansættelsesforhold sjældent har mulighed for frivilligt at afgive sit samtykke, idet der er tale om et over/-underordnelsesforhold, og det derfor er yderst sjældent at et sådant samtykke afgives frivilligt.

Hi3G foreslår, at den kommende databeskyttelseslov ensrettes i forhold til artikel 29-gruppens udtalelser, således at databeskyttelsesloven på dette punkt ikke adskiller sig fra artikel 29-gruppens udtalelse, idet det efter Hi3G's vurdering fortsat må forventes, at samtykke som behandlingsgrundlag ved personaleadministration ikke bør være hovedreglen grundet det særlige over-/underordnelsesforhold.

Hi3G er opmærksom på, at artikel 29-gruppens udtalelser principielt set er vejledende, men der er efter Hi3G's vurdering ikke forhold, der efterfølgende skulle antyde, at artikel 29-gruppens udtalelse skulle have mistet sin aktualitet.

Det foreslås således, at databeskyttelsesloven i forbindelse med behandlingen af personoplysninger i forbindelse med ansættelsesforhold derfor baserer behandlingen af personoplysninger ud fra, at virksomheder kan have en legitim interesse i at behandle sådanne oplysninger, og at behandlingsgrundlaget i stedet baseres med baggrund i afvejningsreglen i medfør af forordningens art. 6, stk. 1. litra f.

Sanktionsspørgsmålet i forhold til offentlige myndigheder § 41, stk. 5.
I lovforslaget fremgår det, at sanktionsspørgsmålet i forhold til offentlige myndigheder er uafklaret.

Hi3G har i forhold til dette spørgsmål imidlertid en række forhold, som selskabet gerne vil bemærke. Hi3G finder, at det bør inddrages i overvejelserne omkring sanktioner til offentlige myndigheder, at der sikres eller skabes et incitament til at offentlige myndigheder på samme vis, som private sikrer, at enhver behandling af persondata overholdes.

Det er Hi3G's vurdering, at der formentlig er en forholdsvis lille risiko forbundet med overtrædelser i forhold til ministerier og styrelser, og øvrige dele af centraladministrationen. Derimod kan der for f.eks. kommuner og regioner være økonomiske forhold eller budgetmæssige forhold, som sammenholdt med manglende sanktioner, kan bevirke, at incitamenterne og dermed prioriteringen af at sikre, at behandling af persondata overholdes ikke har samme bevågenhed, som det ville have haft, hvis der var sanktioner forbundet med manglende overholdelse.

Hi3G finder, at der er behov for at sikre, at der på alle niveauer af den offentlige forvaltning skabes et incitament, som uagtet økonomiske anliggender eller øvrige forhold ikke forårsager, at offentlige myndigheder har mulighed for at nedprioritere databeskyttelse i forhold til behandling af personoplysninger af ressourcemæssige årsager.

Hi3G er opmærksom på, at det forhold at en myndighed giver bøder til en anden myndighed kan virke grundløst, idet der reelt set er tale om at allokere midler fra en kasse til en anden kasse. På trods af dette er der alligevel andre forhold, som kunne tale for, at der alligevel er behov for at skabe det rette incitament til at sikre, at offentlige myndigheder overholder og prioriterer den kommende persondataforordning henholdsvis databeskyttelseslov.

Manglende sanktioner overfor det offentlige kan bevirke, at private virksomheder i deres interaktion med f.eks. kommuner og regioner og øvrige offentlige myndigheder ikke har garantier for, at f.eks. virksomhedernes medarbejderes personoplysninger, som udveksles med de offentlige myndigheder, sikres på behørig vis. En sådan garanti er sanktionsbestemmelser blandt andet med til at understøtte.

Hi3G finder således, at offentlige myndigheders manglende sanktioner kan bevirke, at private ikke opnår de fornødne garantier for, at offentlige myndigheder prioriterer og garanterer tilstrækkelig databeskyttelse i medfør af databeskyttelsesloven såvel som databeskyttelsesforordningen.

Hi3G skal bemærke, at en alternativ løsning kunne være at skabe et incitament for offentlige myndigheder til at overholde databeskyttelsesloven såvel som databeskyttelsesforordningen ved at skabe mere offentlighed omkring offentlige myndigheders overholdelse af lovgivningen. Ved at datatilsynet i højere grad skabte mere offentlighed omkring det offentliges behandling af personoplysninger, kunne der opnås de samme effekter og incitamenter for det offentlige, som der er for det private i forhold til at prioritere databeskyttelse.

Med venlig hilsen

Sebastian Yann Dines
Legal Counsel

Advokatrådet

ADVOKAT SAMFUNDET

Justitsministeriet
Slotsholmsgade 10
1216 København K

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF. 33 96 97 98

DATO: 16. august 2017
SAGSNR.: 2017 - 2003
ID NR.: 475707

databeskyttelse@jm.dk

Høring - over udkast til forslag til databeskyttelsesloven

Ved e-mail af 7. juli 2017 har Justitsministeriet anmodet om Advokatrådets bemærkninger til ovennævnte forslag.

Indledningsvis bemærkes, at Advokatrådet naturligvis har fulgt forhandlingen om - og vedtagelsen af Europa-Parlamentets og Rådets forordning nr. 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) som lovforslaget har til formål at supplere og implementere. Advokatrådet har ligeledes gennemgået Justitsministeriets betænkning nr. 1565/2017 om databeskyttelsesforordningen, hvis analyser har dannet grundlag for lovforslaget.

Advokatrådet kan overordnet tilslutte sig det foreliggende lovforslag.

Det bemærkes dog, at blandt andet sanktionsspørgsmålet i forhold til offentlige myndigheder udestår.

Advokatrådet er af den opfattelse, at der – særlig henset til formålet med databeskyttelsesforordningen og lovforslaget – bør gælde et ligebehandlingsprincip for offentlige myndigheder og private virksomheder. Sanktionering af overtrædelser må antages at virke stærkt adfærdsregulerende, hvorfor offentlige myndigheders overtrædelser allerede af den årsag skal kunne sanktioneres på lige fod med andres overtrædelser. Advokatrådet foreslår derfor, at også offentlige myndigheders overtrædelser skal kunne sanktioneres og at sanktionering skal ske efter fuldstændig de samme principper og retningslinjer, som skal gælde for alle andre pligtsubjekter efter den nye databeskyttelseslov.

Afslutningsvis bemærkes, at man med lovudkastet har valgt den ordning, at databeskyttelsesforordningen er optaget som bilag til loven. Det indebærer, at med Folketingets vedtagelse af lovforslaget bliver forordningens tekst en integreret del af den nye databeskyttelseslov. Imidlertid skal forordninger gælde i deres EU-retlige form og må efter traktaten ikke gennemføres i national ret. Den korrekte

fremgangsmåde må efter Advokatrådets opfattelse derfor være, at forordningen i stedet optages som bilag til lovforslaget, jf. herved Justitsministeriets vejledning om lovkvalitet, s. 22, og § 21 i cirkulære nr. 159 af 16. september 1998 om bemærkninger til lovforslag mv.

Med venlig hilsen

Torben Jensen

Høring over udkast til forslag til databeskyttelsesloven

Den 22. august 2017
Sagsnr. S-2017-456
Dok.nr. D-2017-11539
ds/tas

AKADEMIKERNE

THE DANISH CONFEDERATION
OF PROFESSIONAL ASSOCIATIONS

Nørre Voldgade 29, 2. sal
DK – 1358
København K.

T +45 3369 4040
E ac@ac.dk
W www.ac.dk

LO, FTF og Akademikerne har fra Justitsministeriet modtaget høring over udkast til forslag til databeskyttelsesloven (sagsnr. 2016-7910-0021) og har følgende bemærkninger:

1) Det fremgår flere steder i forslaget (eks. side 153), at forslaget i vidt omfang er en videreførelse af de gældende regler i den nugældende persondatalov, samt at det tilstræbes, at der i videst muligt omfang kan ske behandling i samme omfang, som tilfældet er i dag.

LO, FTF og Akademikerne bifalder, at den gældende retstilstand tilstræbes opretholdt.

2) Persondatalovens § 1, stk. 2, vedrørende lovens anvendelse også for anden ikke-elektronisk systematisk behandling, som udføres for private, foreslås med henvisning til den teknologiske udvikling og bestemmelsens deraf følgende – angiveligt - meget begrænsede anvendelsesområde (forslagets side 160-61) udeladt med lovforslaget.

Dette vil betyde, at ikke-elektroniske personalemapper (rene fysiske personalesager) ikke vil være omfattet af lovens anvendelsesområde.

Det er LO's, FTF's og Akademikernes opfattelse, at der – uanset den teknologiske udvikling generelt – fortsat i et forholdsvis betydeligt omfang anvendes rene fysiske personalemapper uden samtidig elektronisk behandling, i navnlig mindre virksomheder.

På den baggrund vil LO, FTF og Akademikerne foreslå, at loven – ligesom den gældende persondatalov – finder anvendelse på anden ikke-elektronisk systematisk behandling, som udføres for private, herunder ikke-elektroniske personalemapper.

3) Lovforslagets § 2, stk. 1, indeholder henvisning til forordningens art. 5, stk. 1-3. For god ordens skyld bemærkes, at art. 5 kun indeholder stk. 1-2.

4) LO, FTF og Akademikerne finder det positivt, at det med forslagets § 2, stk. 4, fastsættes, at lovforslaget og forordningen gælder for enhver form for behandling af personoplysninger i forbindelse med tv-overvågning, og herunder yderligere, at det materielle regelsæt i persondatalovens kapitel 6 a efter bemærkningerne foreslås videreført.

LO, FTF og Akademikerne skal i samme forbindelse foreslå, at der i bemærkningerne til lovforslagets § 2, stk. 4, henvises til Artikel 29-gruppens WP 249 af 8. juni 2017 som fortolkningsbidrag til forslagets § 2, stk. 4, for så vidt angår specifikt ansættelsesforhold.

5) Lovforslagets § 5, stk. 3, indeholder en bemyndigelsesbestemmelse, hvorefter en minister efter forhandling med justitsministeren kan fastsætte nærmere regler om, at personoplysninger af offentlige myndigheder må viderebehandles til andre formål, end de oprindeligt var indsamlet til, uafhængigt af formålenes forenelighed.

LO, FTF og Akademikerne vil foreslå, at der i bemærkningerne eksemplificeres, i hvilke typesituationer § 5, stk. 3, tiltænkes at blive anvendt.

6) Den nugældende behandlingshjemmel for den offentlige forvaltning og private, for så vidt angår oplysninger om væsentlige sociale problemer og andre rent private forhold i persondatalovens § 8, videreføres ikke med lovforslaget (forslagets side 173 -175).

Det fremgår af lovforslagets s. 174, at "oplysninger om væsentlige sociale problemer og andre rent private forhold … ikke omfattes af forordningens udtømmende liste over følsomme oplysninger i artikel 9", og at "Det er Justitsministeriets vurdering, at behandling af oplysninger om væsentlige sociale problemer og andre rent private forhold fremover skal kunne foretages (alene) på baggrund af behandlingsreglerne i forordningens artikel 6, jf. artikel 5.

Uanset Justitsministeriets vurdering, hvorefter beskyttelsesniveauet for denne kategori af oplysninger angiveligt ikke vil sænkes, forekommer det betænkeligt, at en latent særdeles indgribende behandling af følsomme personoplysninger (herunder oplysninger om en medarbejders positive alkohol- eller narkotikatest, alvorlige familiære problemer og bortvisning fra en arbejdsplads) ikke omfattes af en særregulering, som tilfældet er nu.

På den baggrund vil LO, FTF og Akademikerne foreslå, at oplysninger om væsentlige sociale problemer og andre rent private forhold omfattes af en særregulering svarende til persondatalovens § 8.

7) Reglen i persondatalovens § 13 om forbud mod offentlige myndigheders og private virksomheders automatiske registrering af, hvilke telefonnumre der er foretaget opkald til fra deres telefoner, foreslås udeladt med lovforslaget (side 178).

Bestemmelsen tager sigte på at beskytte ansattes privatliv i forbindelse med benyttelsen af telefoner, som er installeret hos den an-

sattes arbejdsgiver, og fastlægger som sådan rammerne for den notoriske integritetskrænkelse, der kan være forbundet med automatisk registrering.

Justitsministeriets henvisning til, at offentlige og private arbejdsgiver fremover skal overholde reglerne i lovforslaget og forordningen, giver samlet indtryk af, at arbejdsgiveres overvågning af medarbejdernes telefonopkald ikke fremover bør underlægges samme begrænsninger som hidtil. Det bemærkes, at offentlige og private arbejdsgivere også for nuværende selvsagt skal overholde samme regler, navnlig de almindelige behandlingsregler i persondatalovens § 5, der i det hele videreføres i forordningens art. 5.

Videre bemærkes, at forbuddet mod automatisk registrering af medarbejderes telefonopkald efter lovens § 13, stk. 1, 1. pkt., alene kan fraviges efter tilsynsmyndigheden i tilfælde, hvor **afgørende hensyn** til private eller offentlige interesser taler herfor.

Den samme eller en lignende skærpet afvejningsregel samt krav om tilsynsmyndighedens tilladelse vil fremover ikke finde anvendelse på automatisk registrering efter lovforslaget.

LO, FTF og Akademikerne vil på denne baggrund foreslå, at reglen i persondatalovens § 13 om forbud mod offentlige myndigheders og private virksomheders automatiske registrering af, hvilke telefonnumre der er foretaget opkald til fra deres telefoner, videreføres.

8) De i persondatalovens § 8 indeholdte regler, for så vidt angår behandling af oplysninger om strafbare forhold, foreslås opretholdt (forslagets s.185 ff.).

LO, FTF og Akademikerne vil – uanset at den gældende retstilstand foreslås videreført – foreslå, at der som yderligere betingelse for såvel privates som offentlige myndigheders legitime behandling af oplysninger om strafbare forhold, når der foreligger et samtykke (§ 8, stk. 2, nr. 1, og § 8, stk. 3, 1. pkt.), tilføjes, at behandlingen skal være **nødvendig**. Et samtykke bør med andre ord aldrig være tilstrækkelig hjemmel til behandling af oplysninger om strafbare forhold, når behandlingen i det hele er unødvendig.

Samtidig vil LO, FTF og Akademikerne foreslå, at det rum for privates skøn, for så vidt angår behandling uden tilstedeværelse af den registreredes samtykke i forslagets § 8, stk. 3, (nødvendigt til varetagelse af en berettiget interesse, når denne interesse klart overstiger hensynet til den registrerede) samt i videregivelsessituationen uden den registreredes samtykke, jf. forslagets § 8, stk. 4, (videregivelse kan dog ske uden samtykke, når det sker til varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdes) – begrænses væsentligt.

Uanset den foreslåede § 8 alene foreslås videreført for så vidt angår oplysninger om strafbare forhold, vil LO, FTF og Akademikerne foreslå, at reglen i persondatalovens § 8, stk. 3, (bemærkningerne s.

267), videreføres. Det forhold, at reglens anvendelsesområde angiveligt er "udvandet af særlovgivning, der fraviger bestemmelsen, på en lang række områder", og at "Bestemmelsen må derfor anses for at have et yderst begrænset anvendelsesområde", udgør ikke en tilstrækkelig garanti for de registrerede i videregivelsessituationen.

9) Med lovforslagets supplerende hjemmelsbestemmelse i § 12 (bemærkningerne side 275, 1. afs.) tilvejebringes sikkerhed for, at der på såvel det offentlige som det private arbejdsmarked kan behandles personoplysninger som hidtil.

LO, FTF og Akademikerne finder det positivt, at bestemmelsen er indsat som en "helgardering" for at sikre et solidt juridisk grundlag for behandling af personoplysninger på hele det danske arbejdsmarked også fremadrettet.

Lovforslagets § 12, stk. 3, indeholder en kraftig præcisering af, at samtykke, jf. artikel 7, kan anvendes som behandlingshjemmel i ansættelsesforhold. Det er LO's, FTF's og Akademikernes opfattelse, at der i samme forbindelse bør advares mod en generel anvendelse af samtykke som grundlag for behandling i ansættelsesforhold, hvilket da også er bekræftet af den seneste udtalelse fra Artikel 29-gruppen (WP 249). Det fremgår blandt andet af udtalelsen (side 23, pkt. 6.2); "*Employees are almost never in a position to freely give, refuse og revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer*". Det bemærkes yderligere, at samtykke i henhold til artikel 7, navnlig stk. 4, skal være reelt, samt at medlemsstaterne ikke (heller ikke via særregler som hjemlet i artikel 88) kan lempe kravene til et gyldigt samtykke.

LO, FTF og Akademikerne forudsætter, at spørgsmålet om, hvorvidt en given databehandling er hjemlet i en overenskomst eller en generel aftale, efter omstændighederne skal afgøres på baggrund af en udtalelse fra de(n) pågældende overenskomstpart(er) herom.

10) De foreslåede begrænsninger i den dataansvarliges oplysningspligt efter artiklerne 13 og 14 samt indsigtsretten efter artikel 15 i lovforslagets § 22 er særdeles vidtgående.

Det forekommer særligt betænkeligt, at oplysningspligten og indsigtsretten må vige for ikke normerede/eksemplificerede private interesser, jf. § 22, stk. 1, i modsætning til hvad der er tilfældet for de opregnede modstående offentlige interesser i § 22, stk. 2, hvortil bemærkes, at undtagelser for oplysningspligten udtrykkeligt er fastlagt i artikel 13, stk. 4, og navnlig i artikel 14, stk. 5.

Med den foreslåede formulering af § 22, stk. 1, vil der levnes en meget væsentlig skønsmargin for blandt andre den private dataansvarliges modstående interesser. Det vil i sagens natur være op til den dataansvarlige selv at foretage afvejningen mellem egne beskyttelsesværdige interesser og på den anden side den registrere-

des interesser, en vurdering der præsumptivt vil falde ud til den dataansvarliges valg af egne interesser. Med henblik på at klargøre karakteren af de vægtige modstående interesser der, at dømme efter bemærkningerne (s. 296 ff.), sigtes til med bestemmelsen, bør de private interesser, der er oplistet i bemærkningerne side 296, 2. afsnit, indgå i lovteksten alt med henblik på, at en indskrænkning af den dataansvarliges oplysningspligt og den registreredes indsigtsret udelukkende kan ske på grundlag af en konkret afvejning af de modstående interesser, der udtrykkeligt er nævnt i bestemmelsen.

Bemærkningerne nævner som eksempler på tilfælde, hvorunder oplysningspligten og indsigtsretten kan begrænses, "… eksempelvis hvis formålet med indsamlingen forspildes, hvis den registrerede får kendskab til indsamlingen.".

LO, FTF og Akademikerne vil foreslå, at denne specifikke undtagelsessituation eksemplificeres i bemærkningerne.

11) Med forslag til § 26 videreføres en retstilstand, hvorefter advarselsregistre, der har til formål at advare andre mod særligt ansættelsesforhold til en registreret, også fremover vil kræve en forudgående tilladelse fra Datatilsynet (persondatalovens § 50), uanset at der efter forordningen ikke er krav om, at der skal indhentes tilladelse fra tilsynsmyndigheden, forinden iværksættelse af visse typer af behandlinger (bemærkningerne side 215 ff.).

LO, FTF og Akademikerne kan i høj grad tilslutte sig ministeriets opfattelse (bemærkningerne side 217, sidste afsnit), hvorefter brugen af advarselsregistre udgør "indgribende former for behandling af personoplysninger" samt, at "Ulovlige behandlinger på dette område vil kunne medføre alvorlige skadevirkninger for de involverede parter." (bemærkningerne side 218, 1. afsnit).

LO, FTF og Akademikerne vil dog anbefale, at der indføres et generelt forbud mod behandling – og navnlig videregivelse – af artikel 9-oplysninger og oplysninger om væsentlige sociale problemer samt øvrige rent private forhold (som reguleret i persondatalovens § 8) i forbindelse med benyttelsen af advarselsregistre eventuelt således, at tilsynsmyndigheden efter fast praksis fastsætter vilkår herom efter § 26, stk. 4. Den registreredes samtykke som behandlingshjemmel i regi af advarselsregistre må henset til registrenes generelle karakter anses for illusorisk, ligesom behandlingshjemlen i artikel 9, stk. 2, litra b, ikke ses at være relevant for behandlinger i advarselsregistre. Der bør endvidere være forbud mod behandlinger af oplysninger om strafbare forhold – i overensstemmelse med Datatilsynets praksis, jf. Dt.s.J.nr. 200-43-0012 – samt det forhold, at behandlingshjemlerne i art. 6 (samtykke og de følgende nødvendighedskriterier) – som er den relevante behandlingshjemmel, for så vidt angår behandling af strafbare oplysninger, jf. art. 10 – ikke bør være anvendelige for advarselsvirksomhed i forbindelse med ansættelsesforhold.

Det er umiddelbart påfaldende, at persondatalovens § 50, stk. 1, nr. 4, vedrørende krav om Datatilsynets forudgående tilladelse, også

når behandling sker med henblik på erhvervsmæssig bistand ved stillingsbesættelse (rekrutteringsvirksomhed), efter alt at dømme udgår med lovforslaget. Det er ydermere påfaldende, at bemærkningerne end ikke forholder sig til, at stk. 1, nr. 4, ikke videreføres. Ovennævnte citater fra bemærkningerne ad indgribende former for behandlinger samt de mulige skadevirkninger i forbindelse med ulovlige behandlinger er notorisk relevante også ved behandlinger i forbindelse med stillingsbesættende virksomhed.

12) Lovforslagets § 40 er en ordret gennemførelse af forordningens artikel 82. Den regulerer erstatning for materiel og immateriel skade.

Bestemmelsen giver dermed ikke godtgørelse for krænkelse af lovens regler om beskyttelse af den registreredes personlige integritet, der ikke medfører formuetab.

Det er LO's, FTF's og Akademikernes opfattelse, at lovforslaget bør indeholde en bestemmelse herom.

Det bemærkes herved, at erstatningsansvarslovens § 26 er uegnet til at regulere forholdet. Bestemmelsen kræver således, at der foreligger en culpøs krænkelse af en vis grovhed. Denne betingelse begrænser i betydelig grad de tilfælde, hvor der kan tilkendes godtgørelse.

Hertil kommer, at retspraksis opererer med en godtgørelse, der som udgangspunkt skal ligge i størrelsesordenen af 10.000 kr. Dette beløb er efter LO's, FTF's og Akademikernes opfattelse utilstrækkeligt som en genoprettelse af krænkelsen.

13) Det fremgår af lovforslagets § 41, stk. 5, at stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder udestår.

LO, FTF og Akademikerne vil i forbindelse med en endelig afklaring af sanktionsspørgsmålet i forhold til offentlige myndigheder forudsætte, at offentlige myndigheder, når de agerer som arbejdsgivere, skal omfattes af de samme sanktionsbestemmelser, som gælder for private arbejdsgivere.

Med venlig hilsen

Akademikerne FTF LO

Børnerådet

Justitsministeriet
Lovafdelingen
Slotsholmsgade 10
1216 K

25. august 2017
J.nr. 3.0.16/aei/sgh

Børnerådets bemærkninger til § 6 i forslag til databeskyttelseslov

Børnerådet tilslutter sig som udgangspunkt Justitsministeriets forslag om en aldersgrænse på 13 år for samtykke til anvendelse af informationssamfundstjenester, dog med disse bemærkninger:
Danske børn og unge er massivt til stede på en lang række online platforme og sociale medier. Vi ved også, at de er til stede på platforme, de formelt set ikke må være på, som fx de 12-årige på Facebook. Det viser, at restriktioner og forsøg på at regulere dette felt er meget vanskeligt. Faren ved at ignorere eller ligefrem sanktionere, at børn er til stede på platforme, de ikke må være, er, at deres tilstedeværelse og adfærd hemmeligholdes for forældre og andre voksne. Dette betyder, at børnene kan have svært ved at bede om hjælp, hvis de oplever noget ubehageligt, og at voksne har svært ved at engagere sig i børnenes online liv.

Derfor mener Børnerådet, at den bedste beskyttelse af børn i relation til deres online adfærd gives ved at anerkende dem som mediebrugere. En aldersgrænse på 13 år for børns samtykke til anvendelse af informationssamfundstjenester er en del af sådan en anerkendelse.

Dog finder Børnerådet det beklageligt, at anerkendelsen og aldersgrænsen samtidig honorerer industriens kommercielle interesser. Børnerådet henviser her også til forordningens præambelbetragtning nr. 38: Børn bør nyde særlig beskyttelse af deres personoplysninger, eftersom de ofte er mindre bevidste om de pågældende risici, konsekvenser og garantier og deres rettigheder for så vidt angår behandling af personoplysninger. En sådan særlig beskyttelse bør navnlig gælde for brug af børns personoplysninger med henblik på markedsføring eller til at oprette personligheds- eller brugerprofiler og indsamling af personoplysninger vedrørende børn, når de anvender tjenester, der tilbydes direkte til et barn.[1]

Børnerådet savner på denne baggrund en dansk diskussion af, hvorvidt det er muligt at adskille anerkendelsen af de 13-15-åriges egen autoritet som mediebrugere – konkretiseret ved deres

[1] Europa-Parlamentets og Rådets Forordning nr. 2016/679 http://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32016R0679&from=DA

samtykke – og beskyttelsen af den samme gruppe i forhold til kommercielle interesser, såsom dataindsamling.

I Justitsministeriets argumentation for en aldersgrænse på 13 år, fremgår det blandt andet, at "børn i Danmark er i høj grad medievante." Det er korrekt, men medievant er langt fra det samme som at være en kompetent mediebruger. En undersøgelse fra Børnerådet (2014)[2] blandt 2.000 elever i 7. klasse viste, at børnene følte, de havde kontrol over de oplysninger, de delte på nettet. Når de blev spurgt nærmere ind til emnet, viste det sig imidlertid, at en stor gruppe ikke vidste, at de efterlod cookies på nettet eller hvad der skete med deres private oplysninger på de sociale medier, og at de havde svært ved at gennemskue, hvornår noget var markedsføring på nettet. Undersøgelsen viste også, at forældrene ikke interesserer sig tilstrækkeligt for børnenes brug af sociale medier.

Børnerådet anbefaler en massiv indsats i forhold til børn og unges - og deres forældres - digitale dannelse, bl.a. gennem undervisning om digitale rettigheder, databeskyttelse osv. Børnerådet har tidligere peget på en styrkelse Medierådet, der allerede arbejder med feltet og fungerer som videnscenter i EU-regi. Ligesom rådet også har anbefalet et øget fokus på digitale strategier ude i kommunerne, hvor børnene i stigende omgang bliver udstyret med fx iPads, og hvor vi oplever, at blandt andet lærere har brug for at blive bedre klædt på til at bruge de digitale medier i undervisningen samt vejlede børnene i deres egen online adfærd og digitale rettigheder.

Børnerådet står gerne til rådighed for en drøftelse herom.

Med venlig hilsen

Per Larsen
Formand for Børnerådet

Lisbeth Sjørup
Souschef

[2] http://www.boerneraadet.dk/media/77730/Bc3b8rneindblik20nr7_Unge20og20medier.pdf

Vesterbrogad
35A, 4. • 1620 København V • Tlf. 3378 33 00 • brd@brd.dk • www.brd.dk • EAN: 5798000985827 • CVR: 25966376

Justitsministeriet
Databeskyttelseskontoret
Slotholmsgade 10
1216 København K

22. august 2017

Copenhagen Business School
CBS Legal
Solbjerg Plads 3, D1.40
2000 Frederiksberg

Jesper Smedegaard Madsen
Specialkonsulent
jsm.legal@cbs.dk
www.cbs.dk

BEMÆRKNINGER TIL UDKAST TIL FORSLAG TIL DATABESKYTTELSESLOVEN

Copenhagen Business School har haft lejlighed til at gennemgå det fremsendte udkast til forslag til databeskyttelsesloven, og udkastet giver anledning til følgende bemærkninger.

Tilladelse til videregivelse til statistiske eller videnskabelige undersøgelser, udkastet § 10, stk. 3

Udkastet § 10, stk. 3 indeholder en videreførelse af bestemmelse i persondataloven § 10, stk. 3, hvorefter tilsynsmyndighedens forudgående tilladelse skal indhentes, inden at oplysninger videregives til brug for statistiske eller videnskabelige undersøgelser.

Datatilsynet har givet generelle tilladelser til universiteterne til videregivelse til statistiske eller videnskabelige undersøgelser, jf. persondataloven § 10, stk. 3 med en række særlige vilkår, fx, at tilladelsen alene omfatter videregivelse til dataansvarlige etableret i Danmark.

Der er i udkastet til forslag til databeskyttelsesloven ikke nævnt noget om, hvilke overvejelser man har gjort sig i forhold til de eksisterende tilladelser i henhold til persondataloven § 10, stk. 3, herunder hvorvidt eksisterende tilladelser vil kunne videreføres efter ikrafttrædelsen af databeskyttelsesloven.

Copenhagen Business School opfordrer til, at der indsættes en bestemmelse i forslaget til databeskyttelsesloven, der fastslår, at der for så vidt angår tilladelser udstedt i henhold til persondataloven § 10, stk. 3, vil der ikke skulle indhentes en ny tilladelse i henhold til udkastet § 10, stk. 3, men at de eksisterende tilladelser kan fortsætte på uændrede vilkår.

Venlig hilsen

Jesper Smedegaard Madsen
Specialkonsulent

FRIVILLIGRÅDET

CENTER FOR FRIVILLIGT SOCIALT ARBEJDE

Justitsministeriet
Lovafdelingen
Slotsholmsgade 10
1216 København K

Ref: LA/HS
22. august 2017

Vedrørende høring over udkast til databeskyttelsesloven

I forbindelse med høring over udkast til databeskyttelsesloven og den tilhørende persondataforordning skal vi hermed tillade os at komme med nogle betragtninger og spørgsmål om mulige konsekvenser for foreningslivet i Danmark.

CFSA og Frivilligrådet er i løbende kontakt med hundredvis af organisationer og foreninger på det frivillige sociale og det sygdomsbekæmpende område. Spændet går fra meget store organisationer med professionelle sekretariater til lokale foreninger udelukkende drevet af frivillige. Fra alle sider møder vi forståelse for behovet for fælles regler, der giver den enkelte person sikkerhed for, at databehandlingen hos både offentlige myndigheder, virksomheder og organisationer foregår fuldt betryggende. Men vi møder også en usikkerhed i forhold til, hvad reglerne konkret vil betyde for foreningslivet, og om de frivillige foreninger uden personaleressourcer vil være i stand til at leve op til regelsættet. Der er ligeledes tvivl om, hvorvidt frivillige foreninger har et it-setup, der kan understøtte implementeringen.

Vi vil derfor generelt opfordre til, at der i implementeringen af regelsættet tages vidtgående hensyn til forskelligheden inden for organisationsverdenen, og at der i særlig grad tages hensyn til de frivilligt drevne foreninger, således at den nye forordning og lovgivning ikke medfører yderligere administrative byrder for dem. Sådanne administrative byrder gør det erfaringsmæssigt vanskeligere at rekruttere frivillige, bestyrelsesmedlemmer mv. til det frivillige foreningsliv og kan dermed være med til at modvirke den generelle politiske ambition om at styrke foreningslivet og gøre det nemmere at være frivillig.

Helt overordnet opfordrer vi til, at der i det lovforberedende arbejde ses på, hvordan mangfoldigheden af foreninger og organisationer skal forholde sig til den nye lovgivning

Center for Frivilligt Socialt Arbejde
Albanigade 54 E, 1. sal
5000 Odense C

T: + 45 66 14 60 61
E: info@frivillighed.dk
W: www.frivillighed.dk

i forhold til områder som medlemskartoteker, registrering af personfølsomme oplysninger, deling af oplysninger i og på tværs af organisationsenheder. Der er et stort behov for at kunne omsætte lovgivningen til let og forståelig viden for den almindelige frivillige og ansatte i små og store frivillige organisationer.

Ud over opfordringen til at inddrage dette generelle hensyn til det frivillige foreningsliv i overvejelserne i forbindelse med implementeringen af regelsættet har vi nogle få mere konkrete kommentarer, spørgsmål og overvejelser baseret på vores store erfaring med det frivillige foreningsliv i Danmark:

- I EU-forordningens artikel 9, stk. 2 om behandling af særlige personoplysninger står der, at en sådan bl.a. må finde sted, hvis "*Behandling foretages af en stiftelse, en sammenslutning eller et andet organ, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art, som led i organets legitime aktiviteter og med de fornødne garantier, og på betingelse af at behandlingen alene vedrører organets medlemmer, tidligere medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed, og at personoplysningerne ikke videregives uden for organet uden den registreredes samtykke.*" Vi er i den forbindelse dels i tvivl om, hvorvidt foreninger generelt kommer ind under kategorien "*en stiftelse, en sammenslutning eller et andet organ, som ikke arbejder med gevinst for øje*". Endvidere undrer vi os over kravet om, at sigtet skal være af "*politisk, filosofisk, religiøs eller fagforeningsmæssig art*", idet det forekommer os ulogisk, hvis bestemmelsen skal tolkes således, at et religiøst samfund fx godt må registrere, om medlemmer har Diabetes 1 eller Diabetes 2, mens Diabetesforeningen modsat ikke må registrere en sådan oplysning om sine medlemmer.

- Regnes videregivelse af oplysninger om medlemmer og/eller frivillige internt i en organisation som videregivelse af personoplysninger i forordningens forstand? I mange foreninger melder medlemmer sig ind i en lokalforening, der giver oplysningerne videre til en landsorganisation, således at medlemmet også kan modtage relevante tilbud herfra. I andre er det omvendt, så frivillige indmeldes i en landsorganisation, som sender lister til lokale afdelinger. Vil dette blive betragtet som videregivelse af oplysninger til en ekstern part (i nogle tilfælde har landsorganisation og lokalforeningen samme CVR-nummer, men i de fleste tilfælde vil der være tale om forskellige)? Og hvis foreninger videregiver oplysninger om medlemmer til en kommune fx i forbindelse med kontrol af kommunale tilskud, bliver det så betragtet som videregivelse af oplysninger?

- I forlængelse af ovenstående er vi i tvivl om, hvorvidt der skal indgås en formel databehandlingsaftale mellem en lokalforening og en landsorganisation, hvis lokalforeningens medlemsadministrationen foretages af landsorganisationen? Med opmærksomhed på, at den organisatoriske struktur kan være forskellig dvs. nogle lokalforeninger er under-enheder af en landsorganisation. Mens andre er selvstændige foreninger, som har tilsluttet sig en landsorganisation.

- Endelig går vi ud fra, at forordningens artikel 10 om behandling af personoplysninger vedrørende straffedomme og lovovertrædelsen ikke indebærer ændringer i reglerne for og kravene til foreningers indhentning og opbevaring af børneattester?

Vi står gerne til rådighed for yderligere oplysninger og dialog om, hvordan reglerne kan komme til at fungere også for foreningslivet, hvis det ønskes.

Med venlig hilsen

Laura Auken
Centerchef
CFSA

Vibe Klarup
Formand
Frivilligrådet

Justitsministeriet
Slotsholmsgade 10
1216 København K

22. AUGUST 2017

Høringssvar - Udkast til forslag til databeskyttelseslov

DIF
DANMARKS IDRÆTSFORBUND

IDRÆTTENS HUS
BRØNDBY STADION 20
2605 BRØNDBY
DANMARK

T: +45 43 26 26 26
WWW.DIF.DK

Danmarks Idrætsforbund takker for modtagelsen af ministeriets høringsskrivelse vedrørende forslag til databeskyttelseslov og for muligheden for hermed at afgive bemærkninger til det fremsendte udkast.

DIF vil samtidig gerne udtrykke anerkendelse for ministeriets villighed til, forud for denne høringsfase, at drøfte rækkevidden af persondataforordningen med repræsentanter fra DIF og fra udvalgte specialforbund, bl.a. Dansk Boldspil-Union og Dansk Håndbold Forund.

Vi har enkelte bemærkninger til det fremsendte udkast til forslag til databeskyttelseslov.

Før dette dog nogle indledende bemærkninger om organisationen DIF:

Danmarks Idrætsforbund
Danmarks Idrætsforbund er hovedorganisation for organiseret idræt i Danmark. DIF organiserer som paraplyorganisation aktuelt 61 specialforbund med mere end 150 forskellige idrætsdiscipliner. Specialforbundene organiserer de lokale idrætsforeninger, hvor den enkelte udøver har sit medlemskab. DIF er samtidig national olympisk komité.

Dansk Firmaidrætsforbund og Danske Gymnastik- og Idrætsforeninger er andre hovedorganisationer inden for den frivillige idræt. Den kommercielt udbudte idræt er ikke organiseret under idrætternes hovedorganisationer.

DIF organiserer ca. 1.9 mio. foreningsmedlemmer og 470.000 frivillige i ca. 9.000 lokale foreninger. Foreningerne virker på et demokratisk grundlag, hvor medlemmerne er valgbare til foreningens ledelse og bestemmer foreningens virke og drift. Foreningerne er og skal være åbne for medlemskab for enhver borger, der ønsker det. Foreningerne er medlem af de omtalte specialforbund, og specialforbundene er medlem af DIF. Organisationen er således på mange måde opbygget på samme måde som organisationerne på arbejdsmarkedet.

Hovedorganisationerne og foreningerne er almennyttige organisationer. Organisationerne drives alene med det almennyttige formål for øje og genererer ikke et afkast til tredjemand eller til fremmede aktiviteter. Organisationernes og foreningernes status som almennyttige er anerkendt i flere forskellige retlige sammenhænge. Foreningsidrætten er således en del af civilsamfundet på lige fod med f.eks. humanitære organisationer, patientforeninger og natur- og miljøorganisationer.

DIF modtager offentlige tilskud og skal efterleve en række lovbestemte forpligtelser. Organisationen skal bl.a. følge WADA-koden om dopingbekæmpelse, er forpligtet til at bekæmpe matchfixing, og organisationen har tillige etableret en udelukkelsessystem tilknyttet børneattestordningen. Der håndteres selvsagt en række personoplysninger i disse sammenhænge, herunder følsomme oplysninger.

Personoplysninger i organisationen DIF
I organisationen DIF håndteres der personoplysninger på alle organisatoriske niveauer og af ganske varierende karakter, alt vedrørende organisationens helt centrale kerneopgave, afviklingen af idrætsaktiviteterne.

I lokalforeningerne behandles ordinære personoplysninger vedrørende selve medlemskabet og vedrørende idrætsdeltagelsen, typisk kontaktoplysninger, alder, kontingentforhold og spilleberettigelse.

I specialforbundene behandles en mængde ordinære personoplysninger ligeledes knyttet til idrætsdeltagelsen, som kan inkludere oplysninger om f.eks. konkurrencedeltagelse, ranglistepoints, karantæner og andre disciplinære foranstaltninger og i nogle tilfælde også oplysninger om ansættelsesforhold for udenlandske trænere og spillere og whereabouts-oplysninger for topatleter.

I DIF selv behandles ligeledes en række forskellige ordinære personoplysninger knyttet til f.eks. centrale uddannelsesaktiviteter og central pådømmelse af idrætstvister. Derudover behandles ganske følsomme oplysninger i disciplinærsager om doping og matchfixing.

En række af de nævnte personoplysninger udveksles mellem de forskellige organisatoriske led, andre personoplysninger gør ikke. Behandlingen af personoplysninger i organisationen DIF har, som det fremgår varierende baggrund, formål og omfang.

Bemærkninger til udkastet til lovforslag

Som indledende bemærkning vil vi gerne anføre, at medlemskabet af en almennyttig organisation som nævnt er baseret på et interessefællesskab mellem de involverede personer. Organisation og medlem har fælles interesser, og organisationens virke er bestemt af medlemmerne. På denne måde adskiller den medlemsbaserede, almennyttige sektor sig fra andre sektorer, hvor relationerne ofte vil være båret af forskelligt rettede interesser, som f.eks. i forholdet borger og stat, forbruger og erhvervsdrivende eller arbejdstager og arbejdsgiver.

Dette interessefællesskab bør indgå med vægt, når persondataforhold vurderes, særligt rækkevidden af givne behandlingshjemler. Denne betragtning har vel i nogen grad, fundet plads i forordningens art. 9, stk. 2, litra d), men ikke i almindelighed om alle personoplysninger.

Med dette sagt, er vores mere specifikke bemærkninger følgende:

Generelle bemærkninger
Vi noterer os Justitsministeriets opfattelse, hvorefter rækkevidden af behandlingshjemlerne i forordningen på meget lange stræk vil være den samme som efter tilsvarende bestemmelser i gældende persondatalov. Dette gældende i øvrigt både for de umiddelbart anvendelige hjemmelsbestemmelser i forordningen og for de af det foreliggende udkast til lovforslag omfattede.

Det er efter vores opfattelse ganske vigtigt, at dette udgangspunkt fastholdes, også efterfølgende i Datatilsynets praksis. Det er tilsvarende vigtigt, at pådømmelse af regelsættet i de forskellige nationale datatilsyn og ved EU-domstolen ikke

ændrer på den anførte linje, men at denne følges tværnationalt. Der bør således ikke gennem en dynamisk regelanvendelse i EU ske en udvidelse af regelsættets rækkevidde, som ændrer på det nævnte udgangspunkt.

Ordinære personoplysninger – udkastets § 6
Som omtalt behandles der i alle led i organisationen DIF en lang række varierende typer af personoplysninger, lige fra lokalforeningens ordinære medlemsdata til hovedforbundets i nogle tilfælde mere kvalificerede oplysninger.

Det er vigtigt for DIF, at forordningens artikel 6, stk. 1, litra f) vil blive praktiseret på samme måde som interesseafvejningsreglen i gældende persondatalovs § 6, stk. 1, nr. 7. Vi forstår bemærkninger i betænkningen og i lovforslaget sådan, at det er tilfældet.

Følsomme personoplysninger knyttet til idrætsudøvelsen – udkastets § 7
På udvalgte områder behandles der i DIF følsomme personoplysninger. Det er tilfældet i disciplinære sager om doping og matchfixing og ikke mindst i sager under børneattestordningen. Tilsvarende behandler specialforbundene i deres centrale administration af idrætten i nogle tilfælde mere følsomme oplysninger, bl.a. om ansættelsesforhold for spillere og trænere samt om atleters whereabouts.

Det er vigtigt for DIF, at disse behandlinger fortsat kan rummes under forordningens behandlingshjemler, herunder at forordningens bestemmelser vil blive vurderet på samme måde som for tilsvarende interesseafvejningsregler i gældende persondatalov. Vi forstår bemærkningerne i betænkningen og i lovforslaget sådan, at det er tilfældet.

Oplysningspligten i forordningens artikel 13 og 14 – udkastets § 22
Oplysningspligten i artikel 13 og 14 er tæt knyttet til behandlingsreglerne. Som hovedregel er behandlingen af personoplysninger i DIF i dag omfattet af gældende lovs § 28, stk. 2, og § 29, stk. 2, jf. også Datatilsynets vejledning nr. 126, afsnit 2.3.

Det er vigtigt for DIF, at forordningens tilsvarende artikel 13, stk. 4, og 14, stk. 5, kan administreres på samme vis som tilsvarende bestemmelser under gældende ret, jf. anførte vejledning.

Taget på ordet er artikel 13 og 14 meget vidtrækkende, og bestemmelserne udløser en uhyre omfattende orienteringsforpligtelse ved indhentelse af selv de allermest ordinære personoplysninger. Paradigmet i bestemmelserne synes i øvrigt nærmest at være, at behandlingen af personoplysningerne altid foretages til ugunst for personen og mod dennes ønske.

Det fremgår af Justitsministeriets betænkning om forordningen, at de nævnte undtagelsesbestemmelser i forordningen, artikel 13, stk. 4, og 14, stk. 5, ikke vil kunne tillægges helt samme rækkevidde som tilsvarende bestemmelser under gældende lov.

Det kan give anledning bekymring. I organisation som DIF behandles dagligt og hele tiden en lang række forskellige ordinære personoplysninger. Efter artikel 13 og 14 vil enhver, utvivlsomt legitim behandling af selv den mest ordinære personoplysning som udgangspunkt udløse pligt til orientere om alt fra kontaktoplysninger på den dataansvarlige til klagevejledning, indsigelsesret og ret til dataportabilitet. Også blot når en forening opretter et medlemskab med tilhørende kontaktdata, eller når et specialforbund beder en kursist dokumentere sit medlemskab af en forening eller når DIF svarer et specialforbund om valgbarheden for en formandskandidat.

Det vil således blive ganske afgørende, hvordan § 22 i udkastet til forslag vil blive udmøntet i praksis, og vi skal opfordre til, at praksis kommer så tæt på gældende retstilstand som overhovedet mulig. Det fremgik i forbindelse med udgivelsen af betænkningen, at Justitsministeriet vil udstede en vejledning om den registreredes rettigheder i januar 2018, og vi beder om, at dette forhold bliver adresseret i vejledningen.

Behandling af oplysninger om strafbare forhold – udkastets § 8, stk. 3
Det foreslås, at gældende ordning under persondataloven om den snævre adgang for private til at behandle oplysninger om strafbare forhold videreføres. Dette giver ikke i sig selv anledning til bemærkninger fra DIF's side.

I forslagets opretholdes den opfattelse, at oplysninger om straffedomme og oplysninger om strafbare forhold er identiske forhold; en sidestilling, der stammer helt tilbage fra Registerudvalgets vurdering af det oprindelige direktiv bag persondataloven.

Kriteriet strafbare forhold kan være vanskeligt at håndtere som privat organisation. Men vi noterer os betragtningerne i betænkningens afsnit 3.10 om nødvendig kvalificering af et foreliggende forhold, og vi noterer os, at gældende retstilstand søges videreført. Dette bør fastholdes under behandlingen af lovforslaget, og i givet fald har vi ikke yderligere bemærkninger.

Supplerende bemærkninger
Således vores bemærkninger fra Danmarks Idrætsforbund til det foreliggende udkast. Vi bidrager gerne yderligere, herunder i forbindelse med udstedelsen af de kommende vejledninger.

Venlig hilsen

Jan Larsen
Juridisk konsulent

Fra: Charlotte Gundersen DR Jura [CGUN@dr.dk]
Sendt: 21. august 2017 13:00
Til: £Databeskyttelseskontoret (951s26)
Emne: SV: Høring over udkast til forslag til databeskyttelsesloven - (2016-7910-0021) *NDB har en sag/LNJ

Til Justitsministeriet v/Databeskyttelseskontoret

Justitsministeriet har ved mail af 7. juli 2017 sendt udkast til forslag til databeskyttelsesloven i høring.

DR takker for lejligheden til at fremkomme med bemærkninger til forslaget.

DR skal indledningsvis bemærke, at DR finder det positivt, at lovforslaget i videst muligt omfang viderefører de gældende regler i persondatalovens § 2, stk. 2-10.

DR har derfor alene nogle enkelte bemærkninger til lovforslagets § 3.

Af lovforslagets § 3, stk. 1, fremgår, at loven og databeskyttelsesforordningens kapitel II-VII ikke finder anvendelse, hvis det vil være i strid med artikel 10 i Den Europæiske Menneskerettighedskonvention og artikel 11 i Den Europæiske Unions charter om grundlæggende rettigheder. Det ses ikke i bemærkningerne til bestemmelsen at være begrundet, hvorfor området ikke fuldt ud falder uden for loven og databeskyttelsesforordningen, som det i dag er tilfældet efter den nugældende § 2, stk. 2, i persondataloven. Det synes formålstjenligt, såfremt dette uddybes, herunder hvorfor kapitel IX ikke er undtaget cfr. lovforslagets § 3, stk. 5-7.

I bemærkningerne til § 3 er der på side 258, 2. afsnit, henvist til, at forordningens kapitel III vil finde anvendelse. Der bør retteligt stå kapitel VIII. Endelig bør henvisningen til betænkningen, som foretages på side 258 og 259 i lovforslaget være til side 946-956.

Venlig hilsen

Charlotte Gundersen
Juridisk chefkonsulent, DR Jura

DR
DR Byen
Emil Holms Kanal 20, opg. 3-4
DK-0999 København C
T +45 3520 3040
M +45 2854 3664
cgun@dr.dk
http://www.dr.dk

Fra: Justitsministeriet [mailto:jm@jm.dk]
Sendt: 28. juli 2017 10:45
Til: 'post@aabenraa.dk' <post@aabenraa.dk>; Aalborg Kommune – Folkeregisteret <aalborg@aalborg.dk>; 'law@law.aau.dk' <law@law.aau.dk>; 'post@aarhus.dk' <post@aarhus.dk>; 'post@aarhusretshjaelp.dk' <post@aarhusretshjaelp.dk>; 'ekspedition.law@au.dk' <ekspedition.law@au.dk>; 'samfund@advokatsamfundet.dk' <samfund@advokatsamfundet.dk>; 'ac@ac.dk' <ac@ac.dk>; Albertslund Kommune <albertslund@albertslund.dk>; Allerød Kommune <kommunen@alleroed.dk>; 'amnesty@amnesty.dk' <amnesty@amnesty.dk>; 'abf@abf-rep.dk' <abf@abf-rep.dk>; 'ae@ae.dk' <ae@ae.dk>; 'mail@arkitektforeningen.dk' <mail@arkitektforeningen.dk>; 'assens@assens.dk' <assens@assens.dk>; 'pote@atp.dk' <pote@atp.dk>; 'balkom@balk.dk' <balkom@balk.dk>; Beskæftigelsesmin. <bm@bm.dk>; 'kommunen@billund.dk' <kommunen@billund.dk>; 'bl@bl.dk' <bl@bl.dk>; 'post@brk.dk' <post@brk.dk>; 'brondby@brondby.dk' <brondby@brondby.dk>; 'raadhus@99454545.dk' <raadhus@99454545.dk>; Socialmin. <sm@sm.dk>; 'cbs@cbs.dk' <cbs@cbs.dk>; 'bl@bl.dk' <bl@bl.dk>; 'dif@dif.dk' <dif@dif.dk>; 'djoef@djoef.dk' <djoef@djoef.dk>; 'dl@dklf.dk' <dl@dklf.dk>; Journalen [FÆLLESPOSTKASSE] <Journalen@dr.dk>; 'dtu@dtu.dk' <dtu@dtu.dk>; 'da@da.dk' <da@da.dk>; 'info@danskbyggeri.dk' <info@danskbyggeri.dk>; 'de@de.dk' <de@de.dk>; 'hoeringssager@danskerhverv.dk' <hoeringssager@danskerhverv.dk>; 'dfs@dfs.dk' <dfs@dfs.dk>; 'di@di.dk' <di@di.dk>; 'adm@nodeco.dk' <adm@nodeco.dk>; 'dit@dit.dk' <dit@dit.dk>; 'dj@journalistforbundet.dk' <dj@journalistforbundet.dk>; 'info@danske-aeldreraad.dk' <info@danske-aeldreraad.dk>; 'mail@danskeadvokater.dk' <mail@danskeadvokater.dk>; 'cbh@danskeforlag.dk' <cbh@danskeforlag.dk>; 'dh@handicap.dk' <dh@handicap.dk>; 'forening@danskeadvokater.dk' <forening@danskeadvokater.dk>; 'mail@danskemedier.dk' <mail@danskemedier.dk>; 'regioner@regioner.dk' <regioner@regioner.dk>; 'info@danske-seniorer.dk' <info@danske-seniorer.dk>; 'kontakt@danskeudlejere.dk' <kontakt@danskeudlejere.dk>; 'dt@datatilsynet.dk' <dt@datatilsynet.dk>; 'dommerforeningen@gmail.com' <dommerforeningen@gmail.com>; 'dch@dch.dk' <dch@dch.dk>; 'office@voldgiftsinstituttet.dk' <office@voldgiftsinstituttet.dk>; 'dkr@dkr.dk' <dkr@dkr.dk>; $Direktoratet for Kriminalforsorgen <dfk@kriminalforsorgen.dk>; 'hoeringer@dommerfm.dk' <hoeringer@dommerfm.dk>; 'pibr@domstol.dk' <pibr@domstol.dk>; 'post@domstolsstyrelsen.dk' <post@domstolsstyrelsen.dk>; Dragør Kommune <SBK@dragoer.dk>; 'kommune@egekom.dk' <kommune@egekom.dk>; 'info@ejendomsforeningen.dk' <info@ejendomsforeningen.dk>; 'efkm@efkm.dk' <efkm@efkm.dk>; 'mail@envina.dk' <mail@envina.dk>; 'pm@adv-martinelli.dk' <pm@adv-martinelli.dk>; 'evm@evm.dk' <evm@evm.dk>; 'raadhuset@esbjergkommune.dk' <raadhuset@esbjergkommune.dk>; 'experian@experian.dk' <experian@experian.dk>; Faaborg-Midtfyn Kommune <sikkerpost@faaborgmidtfyn.dk>; 'post@fabnet.dk' <post@fabnet.dk>; 'raadhuset@fanoe.dk' <raadhuset@fanoe.dk>; 'favrskov@favrskov.dk' <favrskov@favrskov.dk>; 'kommunen@faxekommune.dk' <kommunen@faxekommune.dk>; 'post@finansogleasing.dk' <post@finansogleasing.dk>; 'fm@fm.dk' <fm@fm.dk>; 'mail@finansraadet.dk' <mail@finansraadet.dk>; 'foa@foa.dk' <foa@foa.dk>; 'forbrugerombudsmanden@kfst.dk' <forbrugerombudsmanden@kfst.dk>; 'fbr@fbr.dk' <fbr@fbr.dk>; 'lsc@ankl.dk' <lsc@ankl.dk>; Statsadvokaten i København <sak@ankl.dk>; 'lcanor@statsforvaltningen.dk' <lcanor@statsforvaltningen.dk>; 'pup@plesner.com' <pup@plesner.com>; 'fp@forsikringogpension.dk' <fp@forsikringogpension.dk>; 'fk@fmf.dk' <fk@fmf.dk>; 'fmn@fmn.dk' <fmn@fmn.dk>; Fredensborg Kommune <fredensborg@fredensborg.dk>; 'kommunen@fredericia.dk' <kommunen@fredericia.dk>; 'raadhuset@frederiksberg.dk' <raadhuset@frederiksberg.dk>; 'post@frederikshavn.dk' <post@frederikshavn.dk>; 'epost@frederikssund.dk' <epost@frederikssund.dk>; 'fsr@fsr.dk' <fsr@fsr.dk>; 'ftf@ftf.dk' <ftf@ftf.dk>; 'furesoe@furesoe.dk' <furesoe@furesoe.dk>; 'sekretatiatet@grundejeren.dk' <sekretatiatet@grundejeren.dk>; 'info@tinganes.fo' <info@tinganes.fo>; Gentofte Kommune

<gentofte@gentofte.dk>; 'kommunen@gladsaxe.dk' <kommunen@gladsaxe.dk>; 'glostrup.kommune@glostrup.dk' <glostrup.kommune@glostrup.dk>; 'raadhus@greve.dk' <raadhus@greve.dk>; 'gribskov@gribskov.dk' <gribskov@gribskov.dk>; 'info@nanoq.gl' <info@nanoq.gl>; Guldborgsund Kommune <jobcenter@guldborgsund.dk>; 'post@haderslev.dk' <post@haderslev.dk>; Halsnæs Kommune <mail@halsnaes.dk>; 'au@au.dk' <au@au.dk>; 'nyhedensted@hedensted.dk' <nyhedensted@hedensted.dk>; 'mail@helsingor.dk' <mail@helsingor.dk>; 'herlev@herlev.dk' <herlev@herlev.dk>; 'kommunen@herning.dk' <kommunen@herning.dk>; 'hillerod@hillerod.dk' <hillerod@hillerod.dk>; 'hjoerring@hjoerring.dk' <hjoerring@hjoerring.dk>; 'hk@hk.dk' <hk@hk.dk>; 'hovedstaden@hk.dk' <hovedstaden@hk.dk>; 'sammail@holbkom.dk' <sammail@holbkom.dk>; 'horsens.kommune@horsens.dk' <horsens.kommune@horsens.dk>; 'hvidovre@hvidovre.dk' <hvidovre@hvidovre.dk>; 'post@hoejesteret.dk' <post@hoejesteret.dk>; Høje-Taastrup Kommune <kommune@htk.dk>; 'kommunen@horsholm.dk' <kommunen@horsholm.dk>; 'hvr@hvr.dk' <hvr@hvr.dk>; 'post@ikast-brande.dk' <post@ikast-brande.dk>; 'isobro@isobro.dk' <isobro@isobro.dk>; 'ida@ida.dk' <ida@ida.dk>; 'info@humanrights.dk' <info@humanrights.dk>; Ishøj Kommune <folkeregister@ishoj.dk>; 'itb@itb.dk' <itb@itb.dk>; 'raadhus@jammerbugt.dk' <raadhus@jammerbugt.dk>; 'info@justitia-int.org' <info@justitia-int.org>; 'kalundborg@kalundborg.dk' <kalundborg@kalundborg.dk>; 'kommune@kerteminde.dk' <kommune@kerteminde.dk>; 'km@km.dk' <km@km.dk>; 'kl@kl.dk' <kl@kl.dk>; 'raadhus@kolding.dk' <raadhus@kolding.dk>; 'info@kreakom.dk' <info@kreakom.dk>; 'info@cancer.dk' <info@cancer.dk>; 'kum@kum.dk' <kum@kum.dk>; 'kobenhavn@domstol.dk' <kobenhavn@domstol.dk>; 'borgerservice@kk.dk' <borgerservice@kk.dk>; 'jurfak@jur.ku.dk' <jurfak@jur.ku.dk>; 'raadhus@koege.dk' <raadhus@koege.dk>; 'pt@strafferetsadvokaten.dk' <pt@strafferetsadvokaten.dk>; 'krim@krim.dk' <krim@krim.dk>; 'vnn.stat@hktillidsvalgt.dk' <vnn.stat@hktillidsvalgt.dk>; 'lo@lo.dk' <lo@lo.dk>; 'post@langelandkommune.dk' <post@langelandkommune.dk>; 'llodk@llodk.dk' <llodk@llodk.dk>; Lemvig Kommune <social@lemvig.dk>; 'kmr@ac.dk' <kmr@ac.dk>; 'lolland@lolland.dk' <lolland@lolland.dk>; Lyngby-Taarbæk Kommune - borgerservice <lyngby@ltk.dk>; 'dadl@dadl.dk' <dadl@dadl.dk>; 'info@lif.dk' <info@lif.dk>; 'kommunen@laesoe.dk' <kommunen@laesoe.dk>; 'raadhus@mariagerfjord.dk' <raadhus@mariagerfjord.dk>; 'middelfart@middelfart.dk' <middelfart@middelfart.dk>; 'mim@mim.dk' <mim@mim.dk>; 'fmn@fmn.dk' <fmn@fmn.dk>; 'kommunen@morsoe.dk' <kommunen@morsoe.dk>; 'nmkn@nmkn.dk' <nmkn@nmkn.dk>; 'norddjurs@norddjurs.dk' <norddjurs@norddjurs.dk>; Nordfyns Kommune <post@nordfynskommune.dk>; 'kommune@nyborg.dk' <kommune@nyborg.dk>; 'borger@naestved.dk' <borger@naestved.dk>; 'odder.kommune@odder.dk' <odder.kommune@odder.dk>; Odense Kommune <odense@odense.dk>; Odsherred Kommune <kommune@odsherred.dk>; 'sekretariat@parcelhus.dk' <sekretariat@parcelhus.dk>; 'lfr001@politi.dk' <lfr001@politi.dk>; 'mail@politiforbundet.dk' <mail@politiforbundet.dk>; 'skrivpost@postnord.com' <skrivpost@postnord.com>; 'post@procesbevillingsnaevnet.dk' <post@procesbevillingsnaevnet.dk>; 'prosa@prosa.dk' <prosa@prosa.dk>; 'randerskommune@randers.dk' <randerskommune@randers.dk>; 'mail@realkreditforeningen.dk' <mail@realkreditforeningen.dk>; 'rkr@rkr.dk' <rkr@rkr.dk>; 'raadhus@rebild.dk' <raadhus@rebild.dk>; 'info@shipowners.dk' <info@shipowners.dk>; 'formand@retspolitik.dk' <formand@retspolitik.dk>; 'aalborg@domstol.dk' <aalborg@domstol.dk>; 'aarhus@domstol.dk' <aarhus@domstol.dk>; 'esbjerg@domstol.dk' <esbjerg@domstol.dk>; 'glostrup@domstol.dk' <glostrup@domstol.dk>; 'helsingor@domstol.dk' <helsingor@domstol.dk>; 'herning@domstol.dk' <herning@domstol.dk>; 'hillerod@domstol.dk' <hillerod@domstol.dk>; 'hjorring@domstol.dk' <hjorring@domstol.dk>; 'holbaek@domstol.dk' <holbaek@domstol.dk>; 'holstebro@domstol.dk' <holstebro@domstol.dk>; 'horsens@domstol.dk' <horsens@domstol.dk>; 'kolding@domstol.dk' <kolding@domstol.dk>; 'lyngby@domstol.dk' <lyngby@domstol.dk>; 'nykobing@domstol.dk' <nykobing@domstol.dk>; 'naestved@domstol.dk' <naestved@domstol.dk>;

'odense@domstol.dk' <odense@domstol.dk>; 'randers@domstol.dk' <randers@domstol.dk>; 'roskilde@domstol.dk' <roskilde@domstol.dk>; 'svendborg@domstol.dk' <svendborg@domstol.dk>; 'sonderborg@domstol.dk' <sonderborg@domstol.dk>; 'viborg@domstol.dk' <viborg@domstol.dk>; 'bornholm@domstol.dk' <bornholm@domstol.dk>; 'frederiksberg@domstol.dk' <frederiksberg@domstol.dk>; 'rigsadvokaten@ankl.dk' <rigsadvokaten@ankl.dk>; 'riomgr@gl.stm.dk' <riomgr@gl.stm.dk>; 'ro@fo.stm.dk' <ro@fo.stm.dk>; 'politi@politi.dk' <politi@politi.dk>; 'post@rksk.dk' <post@rksk.dk>; 'ringsted@ringsted.dk' <ringsted@ringsted.dk>; 'kommunen@roskilde.dk' <kommunen@roskilde.dk>; 'rudersdal@rudersdal.dk' <rudersdal@rudersdal.dk>; Rødovre Kommune <rk@rk.dk>; 'info@digitalsikkerhed.dk' <info@digitalsikkerhed.dk>; 'rem@siri.dk' <rem@siri.dk>; 'slrtv@slrtv.dk' <slrtv@slrtv.dk>; Samsø Kommune <kommune@samsoe.dk>; 'ksm@sikkerhedsbranchen.dk' <ksm@sikkerhedsbranchen.dk>; 'kommunen@silkeborg.dk' <kommunen@silkeborg.dk>; Skanderborg Kommune <skanderborg.kommune@skanderborg.dk>; 'skm@skm.dk' <skm@skm.dk>; Skive Kommune <sk@skivekommune.dk>; 'slagelse@slagelse.dk' <slagelse@slagelse.dk>; 'kommune@solrod.dk' <kommune@solrod.dk>; Sorø Kommune <soroekom@soroe.dk>; 'stm@stm.dk' <stm@stm.dk>; 'stevns@stevns.dk' <stevns@stevns.dk>; 'struer@struer.dk' <struer@struer.dk>; 'sum@sum.dk' <sum@sum.dk>; 'svendborg@svendborg.dk' <svendborg@svendborg.dk>; 'sdu@sdu.dk' <sdu@sdu.dk>; Syddjurs Kommune <syddjurs@syddjurs.dk>; 'post@shret.dk' <post@shret.dk>; 'post@sonderborg.dk' <post@sonderborg.dk>; 'thistedkommune@thisted.dk' <thistedkommune@thisted.dk>; 'ssha@domstol.dk' <ssha@domstol.dk>; 'trm@trm.dk' <trm@trm.dk>; 'jura@tv2.dk' <jura@tv2.dk>; 'toender@toender.dk' <toender@toender.dk>; Tårnby Kommune <kommunen@taarnby.dk>; 'hfa@ac.dk' <hfa@ac.dk>; 'ufm@ufm.dk' <ufm@ufm.dk>; 'um@um.dk' <um@um.dk>; 'uim@uim.dk' <uim@uim.dk>; 'uvm@uvm.dk' <uvm@uvm.dk>; 'raadhus@vallensbaek.dk' <raadhus@vallensbaek.dk>; 'vardekommune@varde.dk' <vardekommune@varde.dk>; 'post@vejenkom.dk' <post@vejenkom.dk>; Vejle Kommune <post@vejle.dk>; 'post@vesthimmerland.dk' <post@vesthimmerland.dk>; 'post@vestrelandsret.dk' <post@vestrelandsret.dk>; 'viborg@viborg.dk' <viborg@viborg.dk>; 'post@vordingborg.dk' <post@vordingborg.dk>; 'aeldresagen@aeldresagen.dk' <aeldresagen@aeldresagen.dk>; 'aef@aeldreforum.dk' <aef@aeldreforum.dk>; 'post@aeroekommune.dk' <post@aeroekommune.dk>; 'oim@oim.dk' <oim@oim.dk>; 'post@oestrelandsret.dk' <post@oestrelandsret.dk>; '3f@3f.dk' <3f@3f.dk>; dfs@dfs.dk; plj@fmf.dk; arsmad@statsforvaltningen.dk; hip001@politi.dk; faglig@prosa.dk
Emne: Høring over udkast til forslag til databeskyttelsesloven - (2016-7910-0021)

Justitsministeriet skal anmode om, at eventuelle bemærkninger til udkast til forslag til databeskyttelsesloven sendes til databeskyttelse@jm.dk.

Med venlig hilsen

Nanna Due Binø
Fuldmægtig

Databeskyttelseskontoret
Slotsholmsgade 10
1216 København K
Tlf. direkte: 72268828
Tlf.: 7226 8400

www.justitsministeriet.dk
jm@jm.dk

DANMARKS STATISTIK

20. juni 2017
BJO
Direktionen

Bemærkninger til ny persondatalov vedr. statistik

Nedenstående generelle principper er centrale for at forstå, at når personoplysninger, der er indsamlet til statistiske eller videnskabelige formål, kun må behandles til disse formål og ikke siden må behandles til andre formål, er hensigten at beskyttelse de registreredes rettigheder. Dette opnås med en videreførelse af Persondatalovens § 10, stk. 2 og 3. Der er tale om grundlæggende internationale principper, og disse bør afspejles i bemærkningerne til den kommende Persondatalov.

Beskyttelse af de enkelte registrerede

Det er kendetegnende for en behandling af personoplysninger, der udelukkende sker "i statistisk eller videnskabeligt øjemed" eller "med henblik på udførelse af statistiske eller videnskabelige undersøgelser", at bearbejdningen af oplysningerne ikke har til formål at danne grundlag for konkrete retlige eller faktiske foranstaltninger over for de enkelte registrerede, men udelukkende til i aggregeret og anonym form at give grundlag for viden om befolkningen og samfundet.

Når behandling af personoplysninger udelukkende sker til statistiske eller videnskabelige formål, gælder udvidede muligheder for at foretage samkøring af registre mv., netop fordi behandlingen ikke har til formål at danne grundlag for konkrete foranstaltninger over for de enkelte registrerede. Af samme grund har de registrerede ikke samme ret til indsigt mv. i de oplysninger, der udelukkende behandles til statistiske eller videnskabelige formål.

Den særlige restriktive regulering af registersamkøringer begrundes først og fremmest med frygten for, at der gennem samkøring af registre, der hver især er oparbejdet med henblik på varetagelse af egne, særskilte formål, gives mulighed for at danne meget tætte profiler af de pågældende enkeltpersoner, hvilket kan udgøre en risiko for krænkelse af deres privatliv. Ofte har de pågældende afgivet oplysninger om dem selv i en bestemt sammenhæng og til et bestemt formål, uden at have en forventning om, at oplysningerne – sammenstillet med andre oplysninger – vil dukke op i en anden sammenhæng og til et andet formål.

Hvis bearbejdningen tillige har til formål at danne grundlag for konkrete tiltag over for de enkelte registrerede, er der ikke tale om en registrering/behandling, som alene finder sted med henblik på statistik eller forskning. Sådanne behandlinger skal foretages i overensstemmelse med de almindelige behandlingsregler og kan dermed ikke være underlagt de samme undtagelser, som gælder for statistiske eller videnskabelige undersøgelser.

Internationale principper og EU's statistiklovgivning

Hvis persondatalovens § 10, stk. 2 og 3 ikke videreføres i samme omfang som i dag, vil den danske lovgivning på dette punkt stride imod FN's principper for officiel statistik, forordningen om europæiske statistikker samt EU's adfærdskodeks for europæisk statistik, og der vil således opstå to regelsæt alt efter om statistikken udarbejdes til europæiske formål (hvilket er hovedparten) eller til nationale formål.

Beskyttelsen af statistiske oplysninger er et grundlæggende princip i FN's principper for officiel statistik[1], hvor det af princip 6 fremgår, at:

> "Individualoplysninger indsamlet af de statistiske institutioner til statistik bearbejdning, hvad enten de kan henføres til fysiske eller juridiske personer, skal behandles fortroligt og må udelukkende anvendes til statistiske formål."

Af forordningen om europæiske statistikker nr. 223/2009, fremgår det af betragtning 27, at:

> "Anvendelse af fortrolige oplysninger til formål, der ikke udelukkende er af statistisk karakter, f.eks. administrative, retlige eller skattemæssige formål eller til kontrol af statistiske enheders forhold, bør være strengt forbudt."

Forordningen bestemmer endvidere i artikel 2, stk. 1, litra e:

> "»statistisk fortrolighed«: beskyttelse af fortrolige data om enkelte statistiske enheder, der tilvejebringes direkte til statistiske formål eller indirekte fra administrative eller andre kilder; anvendelse af de indhentede oplysninger i ikke-statistisk øjemed og uretmæssig videregivelse er således ikke tilladt."

"Fortrolige data" defineres i forordningens artikel 3, litra 7, som:

> "Data, der giver mulighed for direkte eller indirekte identifikation af statistiske enheder og derved afslører individuelle oplysninger. Når det afgøres, om en statistisk enhed kan identificeres, tages der hensyn til alle de midler, som med rimelighed kan tænkes anvendt af tredjemand til at identificeres den nævnte statistiske enhed".

"Statistisk enhed" defineres i forordningens artikel 3, litra 6, som:

> "Basisobservationsenhed, dvs. en fysisk person, en husstand, en økonomisk aktør og andre foretagender, som dataene vedrører."

Af EU's adfærdskodeks for europæisk statistik[2] fremgår det ligeledes af princip 5 om 'statistisk fortrolighed', at:

> "Det skal i alle henseender garanteres, at dataleverandørernes (husholdningerne, virksomhederne, forvaltningerne og andre respondenter) identitet beskyttes, at de leverede oplysninger behandles fortroligt og kun anvendes til statistiske formål."

Jf. i øvrigt *Betænkning nr. 1345*, Behandling af personoplysninger, afsnit 3.5.1.1. Særligt om samkøring (ss. 227-229) og afsnit 3.5.3.5. Behandling af oplysninger i statistisk og videnskabeligt øjemed (ss. 252-259) samt de nævnte EU-retsakter.

[1] Se FN's grundlæggende principper for officiel statistik, tiltrådt af FN's statistiske Kommission den 14. april 1994, samt af FN's generalforsamling ved resolution nr. A/RES/68/261 af 29. januar 2014.
[2] Jf. Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om medlemsstaternes og Fællesskabets statistikmyndigheders uafhængighed, integritet og ansvarlighed (KOM/2005/0217).

DANMARKS STATISTIK

Danmarks Statistik
Sejrøgade 11
2100 København Ø

Tlf. 39 17 39 17
CVR 17150413

dst@dst.dk
www.dst.dk

10. august 2017

Til Justitsministeriet

Høringssvar til forslag til databeskyttelsesloven

Danmarks Statistik takker indledningsvist for muligheden for at komme med bemærkninger til forslag til databeskyttelsesloven (lovforslaget).

Sammenfattende har Danmarks Statistik bemærkninger til følgende to punkter og aspekter af lovforslaget:

1. Omfanget af lovforslagets mulighed for videregivelse af og efterfølgende senere behandling af personoplysninger, der udelukkende er indsamlet til statistiske formål, bør specificeres yderligere

2. Behov for yderligere begrænsning af registreredes rettigheder når indsamling af og behandling af personoplysninger udelukkende sker til statistiske formål

Ovenstående punkter uddybes i nedenstående.

Ad 1. Omfanget af lovforslagets mulighed for videregivelse af og efterfølgende senere behandling af personoplysninger, der udelukkende er indsamlet til statistiske formål, bør specificeres yderligere

For at kunne opretholde muligheden for at producere statistik med samme omfang, kvalitet og de nuværende ressourcer er det vigtigt for Danmarks Statistik, at den nuværende retstilstand for behandling af personoplysninger til statistiske formål opretholdes. Det vil sige, at personoplysninger, der udelukkende behandles med statistiske eller videnskabelige formål, ikke senere kan behandles i andet end statistisk eller videnskabeligt øjemed, jf. princippet i § 10, stk. 2, i den nugældende persondatalov.[1]

Når behandling af personoplysninger udelukkende foregår til statistiske eller videnskabelige formål, gælder udvidede muligheder for at foretage samkøring af registre, netop fordi behandlingen ikke har til formål at danne grundlag for konkrete afgørelser eller foranstaltninger over for de enkelte registrerede. Af samme grund har de registrerede ikke samme ret til indsigt i de personoplysninger, der udelukkende behandles til statistiske eller videnskabelige formål.

[1] Jf. lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.

Den restriktive regulering af registersamkøringer begrundes traditionelt med bekymringen for, at samkøring af registre, som hver især er oparbejdet med henblik på varetagelse af egne, særskilte formål, giver mulighed for at danne meget tætte profiler af de registrerede enkeltpersoner, hvilket kan udgøre en risiko for krænkelse af deres privatliv. Ofte har de pågældende afgivet oplysninger om dem selv i en bestemt sammenhæng og til et bestemt formål, uden at have en forventning om, at oplysningerne – sammenstillet med andre oplysninger – senere vil dukke op i en anden sammenhæng for at blive behandlet til et andet formål.

Når Danmarks Statistik indsamler personoplysninger, er det vigtigt at kunne garantere, at oplysningerne alene vil blive brugt til statistiske formål. Det er Danmarks Statistiks mangeårige erfaring, at denne garanti og transparens sikrer, at der indberettes mere korrekte oplysninger, fordi de enkelte registrerede ved, at der ikke er en risiko for, at de indberettede oplysninger senere bliver behandlet til andre formål.

Yderligere er det værd at bemærke, at oplysninger, der er indsamlet og behandles til statistiske formål, ikke nødvendigvis har en karakter, der gør dem egnede til andre formål. Statistiske oplysninger kan eksempelvis være imputerede, hvilket betyder, at den enkelte personoplysning er beregnet ud fra andre kendte oplysninger. Dette bruges i de tilfælde, hvor indberetning mangler eller er forsinket. Dermed er det ikke sikkert, at den registrerede vil kunne genkende personoplysningen, og oplysningen vil ikke nødvendigvis stemme overens med virkeligheden. Sådanne oplysninger kan dog være fuldt ud brugbare til udarbejdelse af retvisende aggregerede statistiske eller videnskabelige tabeller.

Behandles sådanne imputerede personoplysninger derimod senere til andre formål – eksempelvis til afgørelser på individniveau – vil det kunne føre til fejlagtige afgørelser, der kan få konsekvenser for den enkelte registrerede.

For personoplysninger, der udelukkende er indsamlet til statistiske eller videnskabelige formål, fremgår det blandt andet af databeskyttelsesforordningens[2] artikel 5, stk. 1, litra b, at personoplysninger skal indsamles til udtrykkeligt angivne formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål. Viderebehandling til blandt andet statistiske formål efter databeskyttelsesforordningens artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål.

Det er derfor Danmarks Statistiks vurdering, at personoplysninger, der udelukkende er indsamlet af Danmarks Statistik til statistiske formål, ikke kan videregives til andre formål end statistiske eller videnskabelige.

Danmarks Statistiks tolkning støtter sig endvidere på databeskyttelsesforordningens artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j, samt artikel 6, hvorefter den registrerede må forvente, at når Danmarks Statistik alene indsamler oplysninger med statistiske formål, så vil oplysninger ikke kunne viderebehandles til eksempelvis administrative formål.

Det er Danmarks Statistiks opfattelse, at dette også fremgår af lovforslagets § 10, stk. 2.

For så vidt angår undtagelsen i forhold omfattet af databeskyttelsesforordningens artikel 89, stk. 4, hvorefter videre behandling kan muliggøres, er det Danmarks Statistiks opfattelse, at dette kun vil være i særtilfælde, der enten vil kræve registreredes samtykke eller særlige omstændigheder, herunder

[2] Jf. Europa-Parlamentets og Rådets forordning nr. 679 af 27. april 2016.

hensynet til registreredes vitale interesser, jf. betænkningen til databeskyttelsesforordningen, jf. s. 984[3], samt lovforslagets § 10, stk. 4.[4]

Justitsministeriet bedes bekræfte, at denne tolkning er korrekt.

Forslag til specifikation

Danmarks Statistik tolker lovforslagets § 10, stk. 2, og bemærkningerne hertil, således, at den nuværende retstilstand tænkes videreført, hvilket Danmarks Statistik til fulde støtter op om.

Dette støttes ligeledes op af lovforslagets § 5, stk. 3, 2. pkt., hvoraf det fremgår, at oplysninger, der har gennemgået en statistisk behandling, ikke må viderebehandles til andre formål.

Dog åbnes der i lovforslagets § 1, stk. 3, op for, at særregler i anden lovgivning går forud for reglerne i lovforslaget, så længe de er i overensstemmelse med databeskyttelsesforordningen.

Med henblik på at undgå uklarhed for de registrerede om Danmarks Statistiks fremtidige behandling af deres personoplysninger til statistiske formål, foreslår Danmarks Statistik derfor, at der i § 1, stk. 3, tilføjes en sætning svarende til den i § 5, stk. 3, 2. pkt.

Efter lovforslagets § 1, stk. 3, bør således indsættes et nyt punkt:

"1. pkt. finder ikke anvendelse på § 10."

Ad 2. Behov for yderligere begrænsning af registreredes rettigheder når indsamling af og behandling af personoplysninger udelukkende sker til statistiske formål

I henhold til databeskyttelsesforordningen artikel 89, stk. 2, kan national lovgivning på statistikområdet fastsætte undtagelser til rettighederne, der er omhandlet i artikel 15 (retten til indsigt), 16 (ret til berigtigelse), 18 (ret til begrænsning af behandling) og 21 (ret til indsigelse).

Danmarks Statistik finder det positivt, at lovforslagets § 22, stk. 5, undtager statistiske oplysninger fra databeskyttelsesforordningens artikel 15, stk.1.

Det er imidlertid Danmarks Statistiks vurdering, at oplysninger, der udelukkende er indsamlet til statistiske formål, også bør undtages fra registreredes rettigheder i hele artikel 15, 16, 18 og 21 i databeskyttelsesforordningen.

Danmarks Statistik behandler udelukkende oplysninger til statistiske formål. Som tidligere beskrevet under punkt 1 kan statistiske oplysninger have en karakter, der gør, at den registrerede vil mene, at oplysningerne ikke er korrekte, eksempelvis hvor der er tale om imputerede oplysninger. Eftersom oplysninger, der udelukkende er indsamlet til statistiske formål i henhold til lovforslagets § 10, stk. 2, ikke må videregives til andre formål, vil disse oplys-

[3] Jf. Betænkning nr. 1565 om databeskyttelsesforordningen.

[4] Danmarks Statistik skal bemærke, at Europa-Parlamentets og Rådets forordning nr. 223/2009 om europæiske statistikker fastsætter, at oplysninger, der er indsamlet til statistiske formål, kun må anvendes til statistiske formål, jf. artikel 20 og præambelbetragtning 27 i nævnte forordning. Ligesom tilsvarende principper gælder for FN's grundlæggende principper for statistikker og i andre internationale sammenhænge.

ninger være afskåret fra at blive brugt imod den registrerede. Dette gør, at den registrerede ikke stilles dårligere, selvom statistikområdet også får undtagelser til databeskyttelsesforordningens artikel 16, 18 og 21 under iagttagelse af de betingelser og garantier, der er omhandlet i artikel 89, stk. 1.

Det er Danmarks Statistiks opfattelse, at det vil være uholdbart, hvis en registreret kan kræve, at behandlingen af vedkommendes oplysninger til statistiske formål skal begrænses. Det vil medføre, at der ikke længere kan udarbejdes retvisende statistik.

På statistikområdet behandles oplysninger om hele befolkningen. Dermed vil antallet af mulige anmodninger fra registrerede på baggrund af databeskyttelsesforordningens artikel 15, 16, 18 og 21 kunne blive særdeles omfattende. Som anført overfor vil de oplysninger, som er behandlet udelukkende til statistiske formål, ikke blive brugt til andre formål, herunder til sagsbehandling eller andre administrative formål. Den registrerede har dermed ingen selvstændig interesse i de oplysninger, der indgår i Danmarks Statistiks registre, da formålet med behandlingen allerede klart er fastsat.

Som ligeledes bemærkes i betænkningen til databeskyttelsesforordningen, jf. s. 983, vil statistiske formål indebære, at resultatet af behandling af statistiske formål ikke er personoplysninger, men aggregerede data, og at hverken dette resultat eller personoplysninger ikke anvendes til støtte for foranstaltninger eller afgørelser, der vedrører bestemte fysiske personer.

Undtages de nævnte artikler ikke, vil den registrerede have en berettiget forventning om, at hver anmodning vil blive selvstændigt behandlet af Danmarks Statistik. Da anmodningerne som nævnt ikke er relevant i relation til statistiske oplysninger, herunder aggregerede data, er det på statistikområdet næppe sandsynligt, at de registrerede vil få medhold i anmodningen, men behandlingen af henvendelserne vil kunne beslaglægge betydelige administrative ressourcer hos Danmarks Statistik.

Forslag til specifikation

Databeskyttelsesforordningens artikel 89, stk. 2, giver mulighed for i national lovgivning på statistikområdet at fastsætte undtagelser til rettighederne, der er omhandlet i artikel 15, 16, 18 og 21.

Hvis den danske databeskyttelseslov kun undtager artikel 15, stk. 1, som det nu fremgår af lovforslagets § 22, stk. 5, vil det sende et signal om, at lovgiver eksplicit ikke ønsker at undtage registreredes rettigheder efter databeskyttelsesforordningens artikel 16, 18 og 21 vedrørende behandling af personoplysninger til statistiske formål.

Dette vil som anført have en række uheldige følger, herunder at Danmarks Statistik ikke længere kan udarbejde retvisende statistik.

Med henblik på at spare både de registrerede og det offentlige for betydelige tidsmæssige og økonomiske omkostninger anbefaler Danmarks Statistik derfor stærkt, at oplysninger, der udelukkende er indsamlet til statistiske eller videnskabelige formål eksplicit får de undtagelser, som databeskyttelsesforordningen giver mulighed for, nemlig vedrørende artikel 15, 16, 18 og 21.

Det foreslås derfor, at lovforslagets § 22, stk. 5, ændres til følgende, for så vidt angår Danmarks Statistiks udarbejdelse af statistikker:

"Databeskyttelsesforordningens artikel 15, 16, 18 og 21 finder ikke anvendelse, hvis oplysningerne udelukkende behandles i videnskabeligt øjemed, eller

hvis oplysningerne kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker."

Justitsministeriet
Databeskyttelseskontoret
databeskyttelse@jm.dk

Høringssvar om udkast til forslag til en ny databeskyttelseslov

22. august 2017
AMJ

Dok ID: 107191

For DA er det afgørende, at en ny databeskyttelseslov etablerer et klart og entydigt grundlag for virksomhedernes indsamling, opbevaring, behandling og videregivelse af persondata.

På arbejdsmarkedsområdet håndterer danske virksomheder løbende store mængder af personoplysninger. Det sker bl.a. som led i den almindelige personaleadministration ved ansættelse af medarbejdere, i forbindelse med f.eks. løn, sygdom, ferie, trivsel, arbejdsretlige kontrolforanstaltninger, målinger og performance samt i forbindelse med fratrædelse.

Hele overenskomstsystemet og adgangen til at håndtere sager i det fagretlige system, som er fundamentet i den danske aftalemodel, er afhængig af, at der kan ske en fleksibel, sikker og ubureaukratisk udveksling af personoplysninger mellem aktørerne.

Forslaget til ny databeskyttelseslov viderefører i vidt omfang de eksisterende regler og praksis for udveksling af personoplysninger på arbejdsmarkedsområdet. Forslaget indeholder desuden en ny supplerende hjemmel for håndtering af personoplysninger i det fagretlige system.

DA kan derfor grundlæggende støtte forslaget til en ny databeskyttelseslov.

DA vil i den forbindelse kvittere for den dialog, der har været mellem Justitsministeriet og Beskæftigelsesministeriet og arbejdsmarkedets parter om særlig de overenskomst- og arbejdsretlige problemstillinger i forbindelse med udformning af dels betænkningen om persondataforordningen og forslaget til databeskyttelseslov.

På statistikområdet mener DA, som bl.a. indsamler og udarbejder løn-, ulykkes- og fraværsstatistik for de mere end 24.000 virksomheder, der er medlem af DA's medlemsorganisationer, at forslaget til databeskyttelseslov bør udnytte alle undtagelsesmulighederne i databeskyttelsesforordningen.

Forslaget til ny databeskyttelseslov bygger efter DA's opfattelse på en for snæver opfattelse af, hvilke data der indgår i grundlaget for en statistisk bearbejdning. Der henvises til de mere specifikke bemærkninger nedenfor.

Forslaget til en ny databeskyttelseslov bygger på en EU-forordning. Lovforslaget supplerer på en række områder bestemmelserne i forordningen. Nogle gange henviser man i lovforslaget til bestemmelser direkte i forordningen. Det betyder, at loven umiddelbart bliver svær at håndtere for de medarbejdere,

DANSK ARBEJDSGIVERFORENING
Vester Voldgade 113
DK-1790 København V
Tlf. 33 38 90 00
www.da.dk
CVR 16834017
E-mail da@da.dk

som skal anvende reglerne i praksis på virksomhedsniveau.

DA vil derfor understrege, at der er behov for, at Datatilsynet eller en anden ansvarlig myndighed udarbejder konkrete handlingsorienterede vejledninger, som er særligt møntet på virksomhedernes behandling af personaleoplysninger. Konkrete vejledninger med eksempler vil være med til at understøtte virksomheders mulighed for at overholde de komplicerede regler og forebygge utilsigtede overtrædelser.

Da vejledningerne skal understøtte virksomhedernes mulighed for at forstå og indrette sig på forordningen og de supplerende lovbestemmelser, og da virksomheder forud for, at forordningen træder i kraft, kan have behov for at opdatere eller ændre deres systemer, er det afgørende, at vejledningerne udarbejdes snarest muligt og senest inden udgangen af 2017.

DA noterer sig, at regulering af kravene og rammerne for den nye databeskyttelsesrådgiver baserer sig direkte på forordningens regler. På den måde undgår man, at der kan opstå retsusikkerhed om forholdet mellem forordningens bestemmelser og eventuelt danske gennemførelsesregler. DA støtter derfor den af Justitsministeriet valgte model for den særlige databeskyttelsesrådgiver.

Lovforslaget bygger på en EU-forordning og den fremtidige fortolkning af forordningen vil blive foretaget af det særlige Databeskyttelsesråd og i sidste instans af EU-Domstolen. DA skal derfor opfordre til, at de danske myndigheder prioriterer ressourcer til at påvirke den løbende fortolkning på EU-plan og inddrager arbejdsmarkedets parter, når det drejer sig om fortolkning på det arbejds- og ansættelsesretlige område. Det gælder særlig i relation til arbejdet i Det Europæiske Databeskyttelsesråd.

Konkrete bemærkninger til lovforslaget

De generelle behandlingsregler i §§ 6-8

Behandling af almindelige oplysninger i § 6

For at skabe klarhed om, at der fortsat kan ske behandling af persondata på det ansættelses- og arbejdsretlige område med hjemmel i de almindelige behandlingsregler i § 6, anbefaler DA, at man via eksempler eller med henvisning til betænkningen præciserer i bemærkningerne til § 6, at virksomheder fortsat kan støtte direkte ret på denne behandlingshjemmel, når de behandler oplysninger i forbindelse med ansættelsesforhold og som led i den almindelige personaleadministration. Det gælder også den praksis, der allerede foreligger fra Datatilsynet.

Det bør af samme grund fremgå af bemærkningerne, særligt til § 6, at lovforslagets § 12 indeholder en supplerende hjemmel. Derfor vil der i ansættelsesforhold også kunne behandles personoplysninger inden for rammerne af lovforslagets øvrige behandlingsregler, herunder §§ 6-8, og forordningens behandlingsregler i artikel 6, 9 og 10.

Behandling af følsomme oplysninger i § 7

DA har noteret, at lovforslagets § 7 indeholder en udtømmende liste over personfølsomme oplysninger, og at oplysninger om væsentlige sociale problemer og andre rent private forhold ikke er medtaget i bestemmelsen, da disse oplysninger alene reguleres af databeskyttelsesforordningens artikel 6.

DA finder det positivt, at Justitsministeriet med lovforslagets § 7, stk. 2, sikrer, at det er muligt at behandle følsomme oplysninger i samme omfang som i dag ved at udnytte muligheden for at fastsætte en national regel (i henhold til forordningens artikel 9, stk. 2, litra b), som gør det muligt at behandle følsomme personoplysninger, hvis det er nødvendigt for at overholde den pågældendendes arbejdsretlige forpligtelser.

Strafbare forhold i § 8

DA noterer, at den danske bestemmelse udspringer af persondataforordningens artikel 10, 1. pkt, hvorefter private alene kan behandle oplysninger om strafbare forhold, hvis behandlingen har hjemmel i EU-retten eller national ret.

DA støtter, at den danske særregel i den nuværende persondatalovs § 8 bliver opretholdt i forslag til databeskyttelseslovens § 8, og dermed sikrer en klar hjemmel til at videreføre virksomhedernes muligheder for at indhente og behandle straffeattester og oplysninger om strafbare forhold på samme måde som i dag.

DA noterer, at behandling af f.eks. straffeattester, i lighed med i dag, kan ske uden samtykke, hvis det er nødvendigt for at varetage en berettiget interesse, som klart overstiger hensynet til den registrerede. DA forslår, at der i bemærkningerne til lovforslagets § 8, 2. pkt, tilføjes som eksempel, at det kan være nødvendigt for virksomheder at indhente straffeattester, hvis det er en forudsætning for at varetage det konkrete job.

Behandlingsregler i § 12 om arbejds- og ansættelsesret

Lovforslagets § 12, stk. 1, fastlægger et supplerende behandlingsgrundlag til de generelle behandlingsregler i §§ 6-8, hvorefter både almindelige og følsomme personoplysninger må behandles i forbindelse med ansættelsesforhold, hvis nødvendigt for at overholde arbejdsretlige forpligtelser og rettigheder fastsat i anden lovgivning eller kollektive overenskomster. Desuden kan der ske behandling, hvis den er legitim efter en konkret "interesseafvejning" i § 12, stk. 2.

Det fremgår af bemærkningerne til bestemmelsen, at § 12 har baggrund i forordningens artikel 88, som giver mulighed for at fastsætte nationale behandlingsregler i love og kollektive overenskomster for behandling af både almindelige og følsomme personoplysninger.

DA foreslår, at der i bemærkningerne til lovforslagets § 12, stk. 1, under henvisning til kollektive overenskomster også henvises til DA/LO-aftalen om kontrolforanstaltninger.

I forlængelse af ovenstående bemærkninger angående lovforslagets § 6 finder DA, at det bør fremgå direkte af lovbestemmelsen, at der er tale om en supplerende bestemmelse. Hermed præciseres det, at almindelige behandlinger i forbindelse med personaleadministration, som ikke nødvendigvis udspringer af en "*arbejdsretlig forpligtelse eller rettighed, som fastlagt i anden lovgivning eller kollektive overenskomster*" fortsat kan finde sted, så længe behandlingen har hjemmel i §§ 6-8.

DA vil endvidere foreslå, at der gives eksempler i lovbemærkningerne på behandlinger, som ikke er fastlagt i eller udspringer af anden lovgivning eller kollektive overenskomster, men som udspringer af praksis eller ledelsesretten generelt, som for eksempel brug af medarbejderfotos på intranettet eller brug af en medarbejders e-mailadresse i en vis periode efter medarbejderens fra-

træden.

DA kan tilslutte sig lovforslagets § 12, stk. 3, hvorefter virksomheder kan anvende samtykke som behandlingsgrundlag ved behandling af persondata i forbindelse med personaleadministration, jf. artikel 7. Det valg er ligeledes foretaget i forbindelse med anvendelse af straffeattester efter lovforslagets § 8. Bestemmelsen fastlægger, at samtykke vil udgøre en behandlingshjemmel i ansættelsesretlige forhold, men at det er op til virksomheden at dokumentere, at samtykket er sket udtrykkeligt og frivilligt.

DA har noteret, at den såkaldte artikel 29-gruppe i deres udtalelse om databehandling på arbejdspladsen af 8. juni 2017 har anlagt en fortolkning af mulighederne for at anvende samtykke som behandlingsgrundlag, som er mere snæver i sit anvendelsesområde end lovforslaget.

For at sikre en højere grad af klarhed foreslår DA, at man i lovforslagets bemærkninger til § 12 og særligt stk. 3 henviser til grundlaget i forordningens betragtning (155), hvoraf det fremgår at:

"Medlemsstaternes nationale ret eller kollektive overenskomster, herunder »lokalaftaler«, kan fastsætte specifikke bestemmelser om behandling af arbejdstageres personoplysninger i ansættelsesforhold, navnlig betingelserne for, hvorledes personoplysninger i ansættelsesforhold kan behandles på grundlag af arbejdstagerens samtykke, og i forbindelse med ansættelse, ansættelseskontrakter, herunder godtgørelse for forpligtelser fastlagt ved lov eller kollektive overenskomster, ledelse, planlægning og tilrettelæggelse af arbejdet, ligestilling og mangfoldighed på arbejdspladsen, sikkerhed og sundhed på arbejdspladsen, individuel eller kollektiv udøvelse og nydelse af rettigheder og fordele i forbindelse med ansættelse samt ophør af ansættelsesforhold."

Samtidigt foreslår DA, at de danske myndigheder arbejder for at påvirke artikel 29-gruppen til at nuancere deres opfattelse af brugen af samtykke i ansættelsesforhold – gerne med specifik henvisning til det danske lovforslag.

DA finder, at det er med til at præcisere retsstillingen, når det fremgår af lovforslagets bemærkninger, at medarbejdere har ret til at trække sit samtykke tilbage, men at oplysningerne fortsat kan behandles, hvis brugen af persondata foregår på et andet juridisk grundlag, herunder f.eks. via lovforslagets § 6.

DA skal i den sammenhæng henvise til vores generelle bemærkninger oven for og understrege behovet for, at man hurtigst muligt udarbejder en konkret vejledning til virksomheder om, hvilke vilkår der skal være opfyldt, før de kan anvende samtykke som grundlag for behandling af persondata i et ansættelsesforhold. Gerne med eksempler på, hvornår det kan være gyldigt at behandle oplysninger efter et andet hjemmelsgrundlag ved medarbejderens tilbagetrækning af samtykke.

Behandlingsregler i § 10 om statistik

Lovforslaget indebærer, at der er usikkerhed om den fortsatte mulighed for at anvende personoplysninger i forbindelse med udarbejdelse af statstik.

På den baggrund finder DA, at man i den nye danske persondatalov bør udnytte hjemmelen i artikel 89 med henblik på at skabe større sikkerhed for, at personoplysninger kan anvendes til statistiske formål.

Lovforslagets § 22, stk. 5, bør derfor ændres til følgende:

"Databeskyttelsesforordningens artikel 15, 16, 18 og 21 finder ikke anvendelse,

hvis oplysningerne udelukkende behandles i videnskabeligt øjemed eller til at udarbejde statistikker."

DA's formulering indebærer, at den passage i lovforslaget, hvorefter virksomheder alene kan anvende persondata til statistikformål i "det tidsrum, som kræves for at udarbejde statistikkerne", udgår. Efter DA's opfattelse vil en sådan begrænsning som foreslået gøre det yderst vanskeligt at anvende data til statistikformål.

Den tekniske udvikling har betydet, at statistikproducenterne kan stille services til rådighed for brugerne – også efter selve udarbejdelsen, hvor de kan søge i statistikkens datagrundlag og danne statistiske resultater, der afspejler konkrete behov baseret på egne specifikationer for afgrænsning af statistikken.

Det giver brugeren en langt større nytte af materialet, end det praktisk er muligt at tilvejebringe ved at danne faste tabeller med aggregerede tal ud fra foruddefinerede afgrænsninger, som klassisk eller traditionel papirbaseret statistik typisk har omfattet. Det er vigtigt at betragte individoplysningerne, der ligger til grund for statistikken, som en del af statistikken. Hvis ikke statistikbegrebet udvides i forhold til det begreb, som anlægges i teksten til lovforslaget, vil det betyde, at en betydelig del af det, som i dag opfattes som statistik, ikke længere vil kunne videreføres, eller kvaliteten og statistikformålene vil kunne komme i fare på grund af registerrettighederne.

Samtidig bør der i bemærkningerne ske en præcisering/udvidelse af statistikbegrebet. Det er vigtigt at betragte individoplysningerne, der ligger til grund for statistikken, som en del af statistikken. Hvis ikke statistikbegrebet udvides i forhold til det begreb, som anlægges i teksten til lovforslaget, vil det medføre, at en betydelig del af det, som i dag opfattes som statistik, ikke vil kunne videreføres på samme måde som i dag.

DA's forslag gælder generelt for fremtidig udarbejdelse af statistik i Danmark og omfatter dermed både de statistikker, som udformes af offentlige myndigheder og private aktører som eksempelvis DA. Efter DA's opfattelse vil en manglende udnyttelse af hjemmelsadgangen efter artikel 89 i forordningen indebære, at nogle af de offentlige statistikker, som DA's oplysninger føder ind til, ikke vil kunne udarbejdes.

Indsigtsret og oplysningspligt

DA er enig med Justitsministeriet i, at det vil være uhensigtsmæssigt at give den registrerede en ubetinget oplysnings- og indsigtsret. Ligeledes støtter DA, at Justitsministeriet har valgt at udnytte muligheden for at undtage oplysninger fra oplysnings- og indsigtsretten i § 22. En vid adgang til indsigt og oplysning vil skabe mulighed for misbrug og medføre uforholdsmæssigt store byrder for virksomhederne.

Tilladelse til behandling

DA ønsker at kvittere for, at den generelle anmeldelsespligt i persondatalovens § 43 bliver ophævet.

I henhold til § 26 skal der fremover indhentes tilladelse fra Datatilsynet bla., *"hvis behandlingen af oplysningerne sker med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret."*

Det følger af bemærkningerne, at bestemmelsen tager sigte på, at der skal indhentes tilladelse, før der iværksættes "advarselsregistervirksomhed". Det

fremgår dog ikke nærmere, hvad der menes med denne type "virksomhed".

Grundlæggende bygger forordningen på et opgør med et tilladelsessystem – mod fokus på eget ansvar for at overholde reglerne i egen virksomhed. DA mener på den baggrund, at man bør være tilbageholdende med at indføre adgange til at fastsætte yderligere regler som eksmeplvis i § 26, stk. 3 om, at der forinden iværksættelses af andre behandlinger end de nævnte i § 26, stk. 1, skal indhentes tilladelse fra Datatilsynet.

Kapitel 12 om håndhævelse

Det fremgår af lovforslaget, at de nuværende bødestørrelser vil blive væsentligt forhøjet som følge af den kommende dataforordning. DA noterer i den forbindelse, at strafudmålingen i Danmark fortsat vil bero på domstolenes konkrete vurdering i det enkelte tilfælde af samtlige omstændigheder i sagen, og at det angivne strafniveau derfor vil kunne fraviges i op- eller nedadgående retning, hvis der i den konkrete sag foreligger skærpende eller formildende omstændigheder i henhold til de almindelige regler om straffens fastsættelse i straffelovens kapitel 10. DA noterer samtidig, at Datatilsynet efter forslagets § 42 vil blive bemyndiget efter § 42 til at udstede administrative bødeforelæg i ukomplicerede sager uden bevismæssige tvivlsspørgsmål.

Med den store fokus der har været på de nye forhøjede bødeniveauer, er det efter DA's opfattelse afgørende, at der udarbejdes vejledning med konkrete retningslinjer gerne suppleret med eventuelle bagatelgrænser og konkrete eksempler. På den måde vil virksomheder kunne blive vejledt om deres retsstilling i forbindelse med eventuelle bødeforlæg.

Såfremt vores bemærkninger giver anledning til spørgsmål, står vi naturligvis til rådighed for uddybning.

Med venlig hilsen
DANSK ARBEJDSGIVERFORENING

Sign. Ann Marie Willemoes Jørgensen

DANSK ERHVERV
BØRSEN
DK-1217 KØBENHAVN K
WWW.DANSKERHVERV.DK

T. +45 3374 6000
INFO@DANSKERHVERV.DK

Justitsministeriet
Databeskyttelseskontoret
Att.: Jakob Lundsager
Slotsholmsgade 10
1216 København K

Sendt pr. mail: databeskyttelseskontoret@jm.dk

22. august 2017

Høring over udkast til forslag til databeskyttelsesloven

Dansk Erhverv har med tak modtaget ovenstående høring. Det er hævet over enhver tvivl, at persondataforordningen er en stor udfordring for dansk erhvervsliv og for vores medlemmer, og vi vil derfor gerne indlede med at rose Justitsministeriet for det store arbejde, ministeriet har erlagt i forbindelse med afgivelse af betænkningen samt det foreliggende lovforslag i et forsøg på at komme med afklaringer på de mange tvivlsspørgsmål forordningen rejser, så tidlig som mulig. Såfremt erhvervslivet skal kunne nå at komme i mål med forberedelserne, er det naturligvis vigtigt, at virksomhederne så tidlig som muligt kan forholde sig til, hvordan den danske lovgivning kommer til at se ud. Vi ser nu frem til de mange vejledninger, der ifølge planen skal offentliggøres i løbet af efteråret, og som forhåbentlig vil bidrage med en række praktiske eksempler, som vores medlemmer vil kunne forholde sig til.

Forordningen giver – som anført i høringen- inden for en lang række områder mulighed for nationale særregler. Dansk Erhverv støtter derfor Justitsministeriets vurdering om, at det er nødvendigt, at der fastsættes en generel lov som supplerer reglerne i databeskyttelsesforordningen.

Vores høringssvar berører ikke det ansættelsesretlige og arbejdsretslige område, idet dette koordineres via Dansk Arbejdsgiverforening.

Generelle bemærkninger

Som allerede fremhævet i vores skrivelse til Justitsministeriet af 29. november 2016 er Dansk Erhverv grundlæggende tilhænger af så ens regler som muligt inden for EU på persondatarettens område. Samtidig bør alt for radikale ændringer i forhold til de nugældende regler undgås, såfremt persondataforordningen ikke blokerer for dette. Dansk Erhverv finder, at "opsamlingsloven" har fundet et fornuftigt leje, og vi kan derfor overordnet støtte lovforslaget.

Specifikke bemærkninger

Der er ingen tvivl om, at den største ændring i forhold til de gældende regler, er de øgede sanktionsmuligheder. Selv om bødeniveauet ikke er eksplicit nævnt i høringsmaterialet, skal vi ikke undlade på ny at gøre opmærksom på, at udsigten til et meget højt bødeniveau naturligvis bekymrer virksomhederne. Vi skal derfor gentage vores opfordring til Justitsministeriet om at arbejde

for, at der i EU dannes en udmålingspraksis, der ikke bryder radikalt med den pragmatiske linje, som Datatilsynet gennem årene har lagt – herunder at der i første omgang gives en advarsel inden der idømmes bøder.

Også bøder til det offentlige
Dansk Erhverv har noteret sig, at lovudkastet ikke foreslår, at offentlige myndigheder skal kunne pålægges straf for overtrædelse af databeskyttelsesloven og forordningen, men at dette udskydes til videre politisk drøftelse. Som vi allerede ved forskellige lejligheder har tilkendegivet, er Dansk Erhverv tilhænger af, at det offentlige også skal kunne idømmes bøder eller andre former for mærkbare sanktioner. Jeg henviser til vores føromtalte skrivelse af 29. november 2016.

Eftersom grundtanken i forordningen er, at højne databeskyttelsesniveauet vil det sende helt forkerte signaler, såfremt det offentlige ville blive fritaget for en sanktionering for mangelfuld datahåndtering.

Afskaffelse af krigsreglen
Dansk Erhverv har noteret sig, at den såkaldte "krigsregel" efter persondatalovens § 41, stk. 4, ikke opretholdes. Dette er vi meget tilfredse med, idet bestemmelsen altid har været en stopklods ved IT-leverancer til det offentlige, hvor leverancen indeholdt løsninger, der indebar, at visse services blev leveret fra en adresse uden for Danmark. Det lader dog til, at der efter lovforslagets § 3, stk. 9, kan indføres en tilsvarende bestemmelse ad bagdøren. På dette punkt skaber lovkommentaren ej heller helt klare linjer, og Dansk Erhverv foreslår derfor at lovforslagets § 3 stk. 9 udgår.

Hvis lovforslaget måtte blive vedtaget i dens nuværende form, er det ikke tilstrækkeligt, at ***nye*** systemer kommer på listen før de tages i brug, som det fremgår af bemærkningerne på side 259. Der bør også tages stilling til eksisterende systemer, der allerede driftsafvikles i dag.

Samtykke fra børn/unge til brug af informationssamfundstjenester (sociale medier og apps)
Dansk Erhverv noterer sig med tilfredshed, at Justitsministeriet har lyttet til Dansk Erhvervs opfordring til, at denne aldersgrænse kan sættes ned til 13 år. Det kan oplyses, at der er præcedens for en 13 års aldersgrænse på andre områder– f.eks. aldersgrænsen i det frivillige kodeks for fødevarereklamer, aldersgrænsen for, hvornår man må dele tilbudsaviser ud, ICC's kodeks o.s.v. Sluttelig svarer 13 år til den foreslåede aldersgrænse i Sverige, og vi kan støtte forslaget.

Videregivelse af almindelige personoplysninger til markedsføringsformål
Det er Dansk Erhvervs opfattelse, at en opretholdelse af reglen vil være i strid med direktivet/forordningen. Justitsministeriet er selv inde på denne problemstilling i betænkningen, side 155. Det er vores opfattelse, at samtykkekravet er for vidtgående, og at interesseafvejningsreglen i langt de fleste tilfælde bør føre til, at virksomheden kan nøjes med at ***oplyse*** den registrerede om videregivelsen. Dansk Erhverv kan derfor ikke støtte forslagets § 13 stk.1.

Sikkerhedsbekendtgørelsen

Dansk Erhverv har med tilfredshed noteret sig, at Justitsministeriet er enig i Dansk Erhvervs tidligere udtrykte opfattelse om, at sikkerhedsbekendtgørelsen ikke kan opretholdes efter forordningens ikrafttræden. Som Dansk Erhverv ligeledes tidligere har givet udtryk for, så mener vi, at det er vanskeligt at angive præcise forskrifter for, hvordan sikkerhed opnås i lyset af den hastige udvikling, der er inden for IT. Vi hilser dog en vejledning på dette område velkommen og har noteret os, at den vil blive offentliggjort i december 2017. Dansk Erhverv bidrager gerne med input til vejledningen.

Reglerne om teledata i lov om elektroniske kommunikationsnet og -tjeneste § 31 (køb af teledata)
Dansk Erhverv har med tilfredshed noteret sig Justitsministeriets opfattelse, at de persondatabehandlinger, der fremgår af lov om elektroniske kommunikationsnet og -tjenester, kan videreføres i medfør af forordningens artikel 6, stk. 1, litra c og/eller e, jf. betænkning nr. 1565, del II.

Problemstillingen omkring, hvorvidt teledata som beskrevet i § 31, kan antages at udgøre almindelige kundedata, og dermed er undtaget fra kravet om samtykke ses dog forsat ikke at være behandlet. Dansk Erhverv henstiller til, at der bliver skabt klarhed herom. Datatilsynets tidligere afgørelse fra 2004 (j.nr. 2004-215-0160) er efter vores opfattelse forkert.

Forfatter og journalist reglen i persondatalovens § 2, stk. 9
Dansk Erhverv noterer sig med tilfredshed, at den nuværende bestemmelse i persondataloven rent indholdsmæssigt videreføres i den nye lov, og vi kan derfor støtte dette. Det er dog vores opfattelse, at når der i bemærkningerne til lovforslaget bruges udtrykket "litterær virksomhed" ikke blot skal henvises til skønlitteratur, men ligeledes faglitteratur.

Særregler for databeskyttelsesansvarlige efter artikel 37, stk. 4
Dansk Erhverv har noteret sig, at der ikke lægges op til, at muligheden efter forordningens artikel 37, stk. 4, hvorved der kan fastsættes yderligere nationale regler, udnyttes. Vi ønsker ikke yderligere regler omkring, hvornår virksomheder skal have en databeskyttelsesansvarlig, og kan derfor støtte Justitsministeries tilgang.

Datatilsynets mulighed for at udstede administrative bøder
Dansk Erhverv er generelt modstander af administrative bøder, men anerkender, at bødeforlægsmuligheden kan være praktisk, når der foreligger et klart billede af, hvilke lovovertrædelser der medfører en given bødestørrelse. På nuværende tidspunkt er det dog fuldstændigt uklart, hvordan bødeniveauet vil udvikle sig, og det er derfor vores opfattelse, at der som minimum skal være en 10-årig periode frem til 2028, hvor bøderne alene fastsættes af domstolene.

Med venlig hilsen
Sven Petersen
Erhvervsjuridisk fagchef

DANSK FORFATTER FORENING

DANSKE SKØNLITTERÆRE FORFATTERE

DANSKE FORLAG
Danish Publishers
Børsen DK-1217 København K
Tlf: +45 3315 6688
info@danskeforlag.dk
www.danskeforlag.dk

databeskyttelse@jm.dk

15. august 2017
SB-074-012/cbh

Høring over udkast til forslag til databeskyttelsesloven

Danske Forlag takker for modtagelse af høringsbrev om udkast til forslag til databeskyttelsesloven og har nedenstående bemærkninger.

Det er vigtigt, at man som forfatter har lov til at samle personoplysninger og behandle dem mere eller mindre systematiseret (til brug for f.eks. nøgleromaner eller biografier) uden at skulle være underlagt persondatalovgivningens regler om orientering til datasubjekterne, sletteplig, pligt til at give "aktindsigt" i det registrerede mv.

Det er derfor positivt at notere, at lovudkastet i § 3, stk. 8 indeholder en bestemmelse om, at behandling af oplysninger, som udelukkende sker med henblik på kunstnerisk eller litterær virksomhed, alene er omfattet af databeskyttelsesforordningens artikel 28 og 32.

I tilknytning til ovenstående følger det bl.a. af forarbejderne, at
"Af bestemmelsens *stk. 8, 2. pkt.* følger, at lovens regler ligeledes kun i begrænset omfang finder anvendelse på behandling, som udelukkende sker med henblik på kunstnerisk eller litterær virksomhed. Med udtrykket *litterær virksomhed* sigtes bl.a. til »skønlitterær virksomhed«, f.eks. udarbejdelse af nøgleromaner, se hertil *betænkningen* side 952- 953. http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/betaenkning_nr._1565_del_i_bind_2.pdf"

I betænkningen på side 951 er der henvist til praksis fra Datatilsynet, som i en afgørelse 2002-082-0075 har antaget, at lovbestemmelsen også gælder faglitteratur, fordi de samme hensyn gør sig gældende.

På denne baggrund antager vi, at faglitteratur også fremover vil være dækket, men for at sikre klarhed i loven anbefaler vi, at der i de ovenfor citerede forarbejder også henvises til, at der med udtrykket *litterær virksomhed* også sigtes til faglitterær virksomhed.

Med venlig hilsen

Christine Bødtcher-Hansen	Morten Visby	Jan Thielke
Direktør	Formand	Formand
Danske Forlag	Dansk Forfatterforening	Danske Skønlitterære Forfattere

22. august 2017
KIH
DI-2017-10345

Justitsministeriet
Databeskyttelseskontoret
Slotsholmsgade 10
1216 København K

Dansk Industri
Confederation of Danish Industry

Høring over udkast til databeskyttelsesloven

Justitsministeriet har ved e-mail af 7. juli 2017 anmodet om DI's eventuelle bemærkninger til udkast til forslag til databeskyttelsesloven.

Som følge af at databeskyttelsesforordningen har direkte virkning i Danmark, vil det pågældende lovforslag supplere de vedtagne regler i databeskyttelsesforordningen og ophæve den nugældende danske persondatalov.

Det skal indledningsvis bemærkes, at DI's bemærkninger til lovforslagets bestemmelser af ansættelsesretlig karakter indgår samlet i DA's høringssvar, hvortil der henvises.

Det er DI's generelle holdning, at der bør være så få danske særregler som muligt på persondataområdet. Dette skyldes først og fremmest, at hensynet til en ensartet europæisk harmonisering på området er vigtigt af hensyn til virksomhedernes arbejde med og overholdelse af reglerne. Der er ikke tvivl om, at danske virksomheder både i dag og fremover vil bruge meget store økonomiske ressourcer på at sikre compliance med databeskyttelsesreglerne. I den forbindelse vil nationale særregler på tværs af EU, herunder i Danmark, gøre det mere besværligt og dermed økonomisk ressourcetungt, uden at det positivt bidrager til virksomhederne konkurrencemæssige situation.

Man bør derfor vælge en så indskrænket fortolkning af reglerne ved den danske databeskyttelseslov, og i de få tilfælde, hvor danske særregler gennemføres, opveje dem over for hensynet til konsekvenserne for dansk erhvervsliv og herunder fornødne proportionalitetshensyn.

Ovennævnte gælder ligeledes i relation til de mange bestemmelser, hvor lovforslaget overlader en kompetence til vedkommende ansvarlige minister for nærmere at udfylde lovgivningen på området.

Lovforslaget fastslår i kapitel 10 i forlængelse af Databeskyttelsesforordningen, at det er Datatilsynet, der i Danmark fører tilsyn med behandling af personoplysninger. Foruden tilsynsopgaven lægger DI vægt på, at Datatilsynet prioriterer sin vejledningsopgave over for virksomhederne og sine internationale opgaver i regi af Databeskyttelsesforordningen.

H. C. Andersens Boulevard 18
1787 København V
Danmark

(+45) 3377 3377
di@di.dk
di.dk

CVR: 16 07 75 93

Konkret betyder det, at Datatilsynets løbende skal bruge ressourcer på udarbejdelse og vedligeholdelse af konkret vejledning til virksomhedernes efterlevelse af Databeskyttelsesforordningen. Der er på nuværende tidspunkt en lang række uklarheder om den konkrete forståelse og håndhævelse af en række af Databeskyttelsesforordningens områder. DI imødeser første skridt til afklaring heraf i form af de af Justitsministeriet bebudede 13 første vejledninger, der er annonceret til at blive udgivet fra september 2017 til januar 2018.

Det er dog væsentlig at understrege, at Datatilsynets vejledningsopgave ikke er opfyldt med de 13 vejledninger. Behovet for vejledning af virksomhederne i overholdelse af Databeskyttelsesforordningen er stort. En klar vejledning er særlig vigtigt, når niveauet for bøder og fængsel, der kan udstedes for ikke at overholde Databeskyttelsesforordningen, har det omfang, som det er tilfældet.

Samtidig opfordrer DI til at inddrage virksomhedernes erfaringer i vejledningsarbejdet samt til, at tidsplanen for udgivelse af de første 13 vejledninger overholdes, så vejledningen til virksomhederne ikke udsættes yderligere, da virksomhederne allerede ved overholdelse af tidsplanen gives utilfredsstillende kort tid til at indrette sig på indholdet af vejledningerne.

På samme måde er Datatilsynets internationale opgavevaretagelse på persondataområdet ikke afsluttet med Artikel 29-arbejdsgruppen. Når Artikel 29-arbejdsgruppen konverteres til Det Europæiske Databeskyttelsesråd, ligger der en væsentlig opgave i varetagelsen af blandt andet danske virksomheders interesser i Databeskyttelsesrådet, der får en række beslutningskompetencer, der har direkte virkning i medlemsstaterne, herunder Danmark. En opgave, der bliver større end arbejdet i Artikel 29-arbejdsgruppen, som Datatilsynet i forvejen ikke har haft ressourcer til at dække alle dele af.

DI vil i forlængelse heraf understrege, at det er svært at forestille sig, at Datatilsynet skal kunne varetage disse opgaveområder på tilfredsstillende vis, hvis tilsynet ikke tilføres væsentlige nye ressourcer til de nye opgaver på samme måde, som det allerede er sket i en række af de øvrige medlemsstaters datatilsyn. DI opfordrer derfor til at finde de nødvendige ressourcer dedikeret til hver af disse to opgaver; vejledning og international indsats.

DI's bemærkninger til de specifikke lovbestemmelser

§ 3 – lovens materielle anvendelsesområde

DI støtter, at der i lovforslagets § 3, stk. 9 kun undtagelsesvis gives mulighed for en begrænsning af databehandling på tværs af det indre marked, herunder at visse offentlige it-systemer skal opbevares i Danmark.

Grundlæggende er DI imod denne undtagelse fra den frie konkurrencesituation i det indre marked og så gerne, at § 3, stk. 9 udgik af lovforslaget. Herudover er det DI's opfattelse, at der ikke er belæg for, at en bestemt geografisk placering af data giver større sikkerhed og beslutningskraft over data. Selvom data er fysisk opbevaret i Danmark, er data ikke skærmet fra fremmede landes aktører. DI vil derfor opfodre til, at sikringen af data sker

gennem de allerede eksisterende værktøjer som databehandleraftale og it-sikkerhedstiltag.

Såfremt lovforslagets § 3, stk. 9 alligevel fastholdes som en del af lovforslaget, er det væsentlig, at omfanget af disse data begrænses i lovforslaget, og at der sker en indsnævring af de meget generelle bemærkninger om data, der potentielt alene må opbevares i Danmark.

DI er endvidere opmærksom på, at lovforslaget udvider Databeskyttelsesforordningens område til også af omfatte afdøde (i 10 år). I Databeskyttelsesforordningen fremgår det flere steder, at forordningen ikke bør finde sted på afdøde personer – eksempelvis i præambel 158. Udover det kort beskrevne formål om bevarelse af afdødes eftermæle, fremstår det uklart, hvorfor hele loven og forordningen skal finde anvendelse på afdøde i op til 10 år. DI skal derfor opfordre til, at bestemmelsen udgår af lovforslaget.

§ 4 – lovens geografiske område

Det fremgår af lovforslaget, at det geografiske område for forordningen og loven er sammenfaldende. Der er imidlertid en række virksomheder, herunder danske hosting- og cloudserviceleverandører, som i dag er usikre på den gældende persondataretlige reguleringsterritoriale udstrækning. Dette gælder særlig i den situation, hvor en dataansvarlig i et tredjeland ønsker at benytte en dansk databehandler til behandling af oplysninger om datasubjekter i det pågældende tredjeland, og den danske databehandler benytter hjælpemidler placeret i Danmark. I det omfang den nugældende danske persondatalov finder anvendelse i sådanne situationer, medfører det en stor ulempe for danske virksomheder, som ønsker kommercielt at udbyde databehandler-ydelser til dataansvarlige i tredjelande.

Det fremkommer DI uklart, i hvilket omfang lovforslaget adresserer eller ændrer denne problemstilling, og ønsker derfor klarhed herom.

Det fremkommer endvidere DI uklart, hvorvidt at loven og dens regler som følge af § 4 skal gælde for situationer, hvor danske borgere befinder i udlandet, og hvor behandlingen af personoplysninger udføres for en databehandler eller for en dataansvarlig, som ikke er etableret i DK eller EU. F.eks. ved identitetstyveri fra danske borgere, der er på ferie eller arbejder i udlandet.

§ 5 – behandling af oplysninger

Det fremgår af lovforslagets § 5, stk. 2, nr. 5, at kryptering og pseudonymisering er "garantier", når der sker behandling af personoplysninger.

DI vil gerne understrege, at der ikke kan stilles garantier, blot fordi man anvender kryptering eller pseudonymisering i sin databehandling. Kryptering og pseudonymisering er databeskyttelsesforanstaltninger og it-sikkerhedsforanstaltninger, der kan medvirke til at reducere risici for den registreredes oplysninger.

DI forslår, at § 5, stk. 2, nr. 5 i stedet omformuleres til: " tilstedeværelse af fornødne databeskyttelsesforanstaltninger, som kan omfatte kryptering eller pseudonymisering. ".

§ 6 – informationssamfundstjenester

Det forslås i bestemmelsen, at behandling af personoplysninger om et barn i forbindelse med udbud af informationssamfundstjenester direkte til børn kun er lovlig, hvis barnet er mindst 13 år.

DI støtter denne implementering af retsakten, som balancerer det åbenbare hensyn til barnets mulige deltagelse i denne form for informationstjenester.

§ 10 – statistiske og videnskabelige undersøgelser

Det forslås i bestemmelsen at videreføre muligheden for behandling af følsomme personoplysninger, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og behandlingen er nødvendig af hensyn til udførelsen af undersøgelserne.

DI støtter videreførelsen af denne mulighed for behandling af personoplysninger med henblik på statistiske og videnskabelige undersøgelser, som har stor betydning for mange danske virksomheders udvikling og forretningsmuligheder.

DI støtter desuden den nye foreslåede 10 stk. 4, hvorefter oplysninger, som er behandlet med henblik på at udføre sundhedsvidenskabelig forskning, senere kan behandles i andet end statistisk eller videnskabelig øjemed, hvis behandlingen er nødvendig af hensyn til varetagelsen af den registreredes vitale interesser.

DI skal i den forbindelse særligt henlede opmærksomheden på, at markedsanalyse- og meningsmålingsinstitutterne er særligt afhængige af adgangen til fortsat at behandle personoplysninger, da deres kerneforretning er at udarbejde undersøgelser og statistikker til deres kunder. Som følge af at der justeres i anmeldelsespligten, samtykkereglerne m.m., er der særligt behov for, at der i det kommende vejledningsarbejde indtænkes, hvordan markedsanalyse- og meningsmålingsinstitutterne arbejder, så de fremtidige rammer for deres forretning i forhold til håndtering af data udformes på en sådan måde, at markedsanalyse- og meningsmålingsinstitutternes konkurrenceevne ikke forringes.

§ 11 – cpr-numre

DI støtter forslaget om, at private fremover bør have adgang til at behandle oplysninger om personnumre, når betingelserne i lovforslaget for behandling af følsomme oplysninger er opfyldt. Det bemærkes i forlængelse heraf, at det ligeledes er positivt, at lovforslaget alene opererer med to kategorier af personoplysninger - almindelige personoplysninger og følsomme personoplysninger - og ikke viderefører de tre kategorier af personoplysninger fra persondataloven.

§ 13 - markedsføring

DI vil som udgangspunkt stille spørgsmålstegn ved, om forordningen giver mulighed for den foreslåede regulering på området for markedsføring, og vil derfor opfordre Justitsministeriet til at afklare dette nærmere med Kommissionens juridiske tjeneste.

For så vidt angår den foreslåede regulering støtter DI så klare og udtømmende regler for videregivelse af oplysninger til brug for markedsføring som muligt. Det er vigtigt i forhold til virksomhedernes overholdelse af loven, at lovens bestemmelser, forarbejder og vejledninger angiver de præcise rammer, som virksomhederne skal agere indenfor. Det er herudover ikke DI's opfattelse, at det bør være et selvstændigt mål, som anført i bemærkningerne, at rammerne for videregivelse til brug for markedsføring skal være så snævre som muligt.

DI finder det på denne baggrund derfor problematisk, at justitsministeren i lovforslaget gives en hjemmel til at fastsætte yderligere ikke definerede begrænsninger i adgangen til videregivelse til brug for markedsføring. DI forslår derfor, at denne mulighed udgår af bestemmelsen.

§ 25 – akkreditering af certificeringsorganer

DI støtter forslaget om, at Justitsministeriet fremover har mulighed for at akkreditere certificeringsorganisationer og afventer den nærmere praktiske implementering af bestemmelsen.

§ 26 – advarselsregistre

Det forslås i bestemmelsen at opretholde en forudgående tilladelse fra Datatilsynet inden iværksættelse af advarselsregistre, på trods af at forordningen ikke kræver en sådan tilladelse.

Der vil på flere områder i dag være et behov for, at virksomheder kan advare hinanden mod svindel mv. i forhold til f.eks. låne- og ansættelsesforhold. Denne mulighed bør ikke unødigt besværliggøres ved at afvente tilladelse fra Datatilsynet. Det er det klare udgangspunkt i forordningen, at det er de involverede virksomheders ansvar at forordningen overholdes, hvilket ligeledes er begrundelsen for at anmeldelsessystemet ikke er en del af kravene i forordningen.

DI kan derfor ikke støtte, at der skal indhentes en forudgående tilladelse til behandling i forbindelse med advarselsregistre.

§ 29 – Datatilsynets adgang til virksomheder

Det forslås i bestemmelsen, at Datatilsynet fremover skal have adgang til **alle** lokaler, hvorfra en behandling af personoplysninger foretages, uden at skulle fremskaffe en retskendelse. I den nuværende udformning af loven har tilsynet kun adgang til lokaliteter uden retskendelse, hvor der behandles oplysninger for den offentlige forvaltning, eller hvor behandlingen kræver forudgående anmeldelse og tilladelse fra Datatilsynet. Denne

markante udvidelse af området, hvor der ikke længere kræves retskendelse, fra særlige begrundede lokaliteter til nu reelt alle danske virksomheder, virker retssikkerhedsmæssigt krænkende.

Lovforslagets bemærkninger begrunder denne udvidelse med henvisning til forordningens artikel 58 litra f), hvorefter tilsynet skal have adgang til alle lokaler i overensstemmelse med retsplejeregler i EU-retten eller medlemsstaternes nationale ret. Forordningen giver således styrelsen hjemmel til en adgang til alle lokaliteter, men lader det stå åbent, på hvilket grundlag de nationale myndigheder har denne adgang med en henvisning til nationale retsplejeregler.

Det klare udgangspunkt i dansk retspleje er, at myndighedsundersøgelser af privates lokaliteter kun kan ske ved indhentelse af retskendelse. Det er ligeledes tilfældet i meget særlovgivning, herunder konkurrencelovens regler, hvor myndighedernes kontrolundersøgelser for konkurrenceovertrædelser kun kan foretages mod behørig retskendelse.

På den baggrund og under hensyntagen til de foreslåede generelle strafskærpelser i lovforslaget, bør tilsynet ikke tildeles denne udvidede adgang til alle danske private lokaliteter uden nogen form for retskendelse.

§ 36 – gebyr for ansøgninger

Ifølge lovforslaget gives justitsministeren nu hjemmel til frit at fastsætte regler om betaling af gebyr for indgivelse af ansøgning om tilladelser i henhold til loven og gebyret størrelse. I den nuværende lov er området og niveauet for betaling af gebyr helt klart fastlagt. DI kan ikke støtte en ændring, hvor det frit overlades til ministeren at fastsætte gebyrområder og gebyrstørrelser for alle danske virksomheder, og skal derfor opfordre til, at den nuværende bestemmelse herom i persondataloven fastholdes.

§ 41 – fængsel

Det forslås i lovforslaget, at man kan straffes med bøde eller fængsel indtil 6 måneder for overtrædelse af en række af lovforslagets bestemmelser. Der henvises som begrundelse for indførsel af en 6 måneders fængselsstraf til straffelovens § 264 d. I lov om retshåndhævende myndigheders behandling af personoplysninger, lov nr. 410 af 27/4 2017, fremgår det af lovens § 50, at en privat databehandler, der udfører en behandling for en offentlig myndighed, og som overtræder loven, kan straffes med fængsel i indtil 4 måneder.

Efter DI's opfattelse virker det naturligt, at en sanktionsbestemmelse i dette lovforslag harmonerer med strafbestemmelsen i lov nr. 410, og forslår derfor indførsel af en straframme på 4 måneder i stedet.

Herudover savnes mere detaljerede bemærkninger om de enkelte strafsubjekter i den enkelte organisation, herunder også i det offentlige jf. lovforslagets § 41 stk. 5.

Endelig udestår en mere detaljeret beskrivelse af sammenhængen mellem fængselsstraf og bødeniveauet.

§ 41 stk. 5. – bøder til offentlige myndigheder

Det fremgår af lovforslaget, at stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder udestår. Dette på trods af, at offentlige myndigheder på tilsvarende måde som private virksomheder er omfattet af lovens forpligtigelser, og på mange områder i dag udøver erhvervsmæssige aktiviteter i konkurrence med private aktører.

DI er derfor af den opfattelse, at offentlige myndigheder på tilsvarende måde som f.eks. i konkurrenceloven, bør ligestilles med private virksomheder ved bødesanktionering i forbindelse med udøvelse af erhvervsmæssig aktivitet. Dette vil både sende et tydeligt signal til offentlige myndigheder om vigtigheden i overholdelsen, og helt grundlæggende ligestille offentlige myndigheder og private virksomheder.

Samtidig bør der ligeledes være passende sanktioner, når offentlige myndigheder i deres øvrige myndighedsudøvelse ikke overholder Databeskyttelsesforordningen. Offentlige myndigheder behandler personoplysninger i et meget stort omfang, og der har i offentligheden været flere eksempler på, at offentlige myndigheder ikke har været foretaget de nødvendige foranstaltninger til beskyttelse af personoplysninger, som de vil være forpligtet til med Databeskyttelsesforordningen. Det er derfor svært at se forordningens hensigt om at beskytte de registreredes grundlæggende rettigheder blive understøttet, såfremt der ikke også sker en sanktionering af offentlige myndigheders overtrædelser af forordningen.

§ 42 – bødeforlæg

Det forslås i lovforslaget at udstede bødeforlæg i tilfælde, hvor den som har begået overtrædelsen har erklæret sig skyldig i overtrædelsen. Det fremgår af lovforslagets bemærkninger, at kompetencen er begrænset til tilfælde, hvor sagen er egnet hertil, dvs. i ukomplicerede sager, hvor der ikke er bevismæssige tvivlsspørgsmål.

DI er grundlæggende skeptisk over for indførsel af muligheden for administrative myndigheder til at udstede bødeforlæg som sanktionsmulighed. Dette skyldes primært, at det i praksis har vist sig svært at sætte grænser for hvilke sager, der kan kategoriseres som ukomplicerede og ikke indeholdende retlige tvivlsspørgsmål. Denne vurdering bør derfor tages af domstolene og ikke af administrative myndigheder som Datatilsynet.

Såfremt bødeforlæg alligevel fastholdes på dette område, bør muligheden i bemærkningerne indsnævres til de situationer, hvor anklagemyndigheden først har vurderet sagen, og der er etableret en helt fast retspraksis, som det f.eks. er tilfældet i konkurrencelovens anvendelse af bødeforlæg.

Med venlig hilsen

Kim Haggren
Underdirektør

Adam Lebech
Branchedirektør

Fra: Pia Ravn [pr@danskkiropraktorforening.dk]
Sendt: 21. august 2017 13:03
Til: Justitsministeriet
Emne: Høring over udkast til forslag til databeskyttelsesloven *NDB har en sag/LNJ

Justitsministeriet
Databeskyttelseskontoret

Dansk Kiropraktor Forening har modtaget høring over forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

DKF har ingen bemærkninger til det fremsendte forslag.

Med venlig hilsen
Pia Ravn

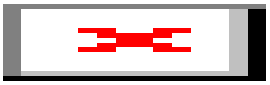
Dansk Kiropraktor Forening
Peter Bangs Vej 30
2000 Frederiksberg
Tel: +45 33930400
Direkte: +45 33376097
www.danskkiropraktorforening.dk

Fra: Charlotte Broe [cb@danske-aeldreraad.dk]
Sendt: 25. august 2017 14:14
Til: £Databeskyttelseskontoret (951s26)
Emne: Danske ældreråd

DANSKE ÆLDRERÅD takker for muligheden for at afgive høringssvar og har ingen bemærkninger.

Med venlig hilsen

Charlotte Broe



DANSKE ÆLDRERÅD
Jernbane Allé 54, 3. th.
2720 Vanløse

Tlf: 38 77 01 60
Dirkte tlf: 38 77 01 67
Mail: cb@danske-aeldreraad.dk

Justitsministeriet

Lovafdelingen

Att. Databeskyttelseskontoret

Tirsdag den 21. august 2017

HØRINGSSVAR

Sagsnr. 2016-7910-0021 – udkast til forslag til databeskyttelsesloven

Brancheforeningen Danske Bedemænd fremsender på vegne af vores 280 medlemsforretninger hermed høringssvar til det kommende lovforslag om ændringer i databeskyttelsesloven.

Indledningsvis skal vi påpege, at vores medlemmer (bedemænd) er alle uddannede bedemænd og at flere af disse endvidere er ISO 9001 certificerede. Dette indebærer bl.a. at vi stiller høje etiske krav til vores medlemmer i forhold til deres virke. Disse etiske krav og for manges vedkommende tillige ISO certificerede procedurer medfører, at personlige data behandles med meget stor omhu og omhyggelighed med henblik på undgåelse af fejl og forbytninger særligt i forhold til afdøde personer, urner, kister etc., men tillige i forhold til behandling af personlige informationer vedr. pårørende til afdøde.

Bedemændene er sammenfattende en meget væsentlig aktør i håndteringen af de i Danmark ca. 53.000 dødsfald pr. år. I relation til hvert enkelt dødsfald skal der være en 100% sikkerhed for, at den nedsatte urne og eller nedsatte kiste rent faktisk indeholder den pågældende afdøde person.

Med baggrund heri er det klart og tydeligt, at der skal være en mulighed for SIKKER identifikation af afdøde undervejs i alle de handlinger, der foretages i forbindelse med et registreret dødsfald.

Én af de sikre og anvendte identifikationsmetodikker indebærer anvendelse af afdødes CPR-nummer, idet dette fremgår såvel af dødsattest, øvrige attester og dokumenter i forbindelse med dødsfaldet samt ikke mindst, at der stilles krav om, at alle afdøde i Danmark skal ilægges kiste og at disse kister SKAL forsynes med tydelig mærkat udvisende afdødes CPR-nummer og navn.

Umiddelbart kan følgende opgavetyper nævnes i relation til høringen og det faktum, at eks. CPR-nummeret anvendes som sikker identifikation i relation til dødsfald:

- Håndtering af dødsattesten inkl. sikre fremskaffelse heraf til begravelsesmyndigheden
- Kontakt til krematorium
- Kontakt til kapel
- Kontakt til udfærdigende læge f.s.v. angår dødsattesten
- Kontakt til Udbetaling Danmark
- Kontakt til Skifteretten
- Kontakt til embedslæger bl.a. for udstedelse af ligpas
- Kontakt til evt. bobestyrer/advokat
- Kontakt til Anatomiske Institutter (Kbh, Odense og Århus)
- Kontakt til Politiet (mistænkelige og/eller strafbare forhold – retslægelige ligsyn/obduktioner)
- Kontakt til kommunen (særligt hvor det offentlige afholder omkostningerne)
- Kontakt til kirkegården for urnenedsættelse / begravelse
- Montering af label/etiket på kisten med afdødes navn, CPR-nummer, dag og klokkeslæt for begravelsen/bisættelsen.
- Sikker mærkning af urne med CPR-nummer
- Hjælp til pårørende i forhold til kontakt til pensionsselskaber, fagforeninger m.v.
- Kontakt til sundhedspersonale på plejecentre, sygehuse, hospice m.v.
- I forbindelse med hjemtransport fra udlandet
- I forbindelse med udtransport til afdødes hjemland
- Generel håndtering af afdødes kiste/urne med henblik på placering på rette lokation eks. kirke/kapel/kirkegård/gravsted/borgerlig højtidelighed etc.
- For nulevende og afdøde:
    - Registrering af Min Sidste Vilje / indhentning af vide om MSV
    - Oprettelse af begravelsesopsparing Elysium / forespørgsel på opsparing og udbetaling herfra jf. godkendelse af Skat og Erhvervsministeriet

Megen kommunikation og udveksling af data foregår i dag elektronisk, dog skal eksempelvis dødsattesten fortsat printes, idet en papirversion af dødsattestens side 1 skal medfølge liget. Med førnævnte oplistning har vi forsøgt uden nærmere definering at anskueliggøre de mange aspekter i en bedemandsforretnings virke, hvor der anvendes personlige oplysninger herunder i form af CPR-numre. Skærpelser i forhold til håndtering af CPR-numre vil derfor uvilkårligt påvirke disse bedemandsforretningers daglige virke og vanskeliggøre den samfundsnyttige opgave, som bedemændene løser.

Bedemænd i Danmark udøver ofte ”halve myndighedsopgaver” eksempelvis når der desværre fortsat sker manglende elektronisk registrering af dødsfald. Bedemanden er her nødsaget til at opsøge pågældende læge, der har udstedt dødsattest og få denne videreformidlet til begravelses-myndigheden (præsten) førend selve begravelseshandlingen kan foregå. Bedemanden fungerer tillige som bindeleddet til skifteretten og bobestyrere med henblik på videreformidling af oplysninger vedr. afdøde.

Hos vores medlemmer og ved bedemænd generelt er det meget udbredt, at familier ved efterfølgende dødsfald kontakter den samme bedemand for at sikre, at også denne nye ceremoni kan foregå som den seneste. Dette være sig i forhold til kistevalg, sange i kirken, ligklæder o.s.v. Hertil benytter bedemanden sig af det oprindelige aftalegrundlag ved den første begravelseshandling, da de pårørende siger, at det skal være ligesom sidst (uagtet sidst kan være for nogle år siden) Bedemænd opbevarer derfor ofte af hensyn til de pårørende disse oprindelige aftalegrundlag i en længere periode.

Med henvisning til EU-forordningens pkt. 39, hvori det nævnes, at ”perioden for opbevaring af personoplysningerne ikke er længere end strengt nødvendigt” kan dette med baggrund i justitsministeriets forslag til ny databeskyttelseslov give bedemændene problemer i forhold til at opbevare disse aftalegrundlag hvad enten det foregår elektronisk og/eller i hard-copy.

Henset her til bør afdøde skrives ud af den danske databeskyttelseslov.

Artikel 87 i forordningen: ”Medlemsstaterne kan nærmere fastsætte de specifikke betingelser for behandling af et nationalt identifikationsnummer eller andre almene midler til identifikation…….”

- Dermed kan Danmark i en række af de love og bekendtgørelser m.v. der er angivet i justitsministeriets betænkning nr. 1565 (Del II – de enkelte ministeriers ressort i henhold til de respektive lovgivninger) fastsætte lempelser og/eller skærpelser.

I høringsudkastet til ny databeskyttelseslov er der i lovforslaget § 2 stk. 5 og 6 lagt op til, at afdøde omfattes af databeskyttelsesloven i en 10-årig periode med mulighed for en længere eller kortere periode.

EU-forordningen 2016/679 af 27. april 2016 anlægger bl.a. følgende betragtning:

Oprindelige forordning og lovforslaget side 29:

(27) "Denne forordning finder ikke anvendelse på personoplysninger om afdøde personer. Medlemsstaterne kan fastsætte regler for behandling af personoplysninger om afdøde personer."

(Engelsk udgave: "*This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons*")

Det fremgår dermed meget klart, at afdøde personers oplysninger IKKE er tiltænkt omfattet af forordningen, og at det i givet fald alene vil bero på den enkelte medlemsstats ønske herom.

Oprindelige forordning og lovforslaget side 68:

(158) "Når personoplysninger behandles til arkivformål, bør denne forordning også gælde for den pågældende behandling, i**det denne forordning dog ikke bør finde anvendelse på afdøde personer."**

Tilsvarende er nævnt i pkt. (160) side 68

Lovforslaget side 153:

Vi er meget uforstående overfor, at vi i Danmark skal skærpe reglerne og dermed gå langt videre end forordningen er tiltænkt, idet I her foreslår, at lovforslaget skal finde anvendelse på afdøde personer i 10 år!!!! *Der vil i givet fald være tale om endnu en dansk overimplementering af en EU-forordning.*

Brancheforeningen Danske Bedemænd
Engelsborgvej 52 . 2800 Kgs. Lyngby . Telefon 45 93 14 11
www.bedemand.dk . Mail: kontakt@bedemand.dk

Lovforslaget side 157:

Vi har delvist forståelse for, at der for visse afdøde kan være hensyn set i relation til helbredsforhold, politisk overbevisning eller strafbare forhold, der kan kræve særlig beskyttelse eks. friholdelse fra regler om aktindsigt etc. Som vi sluttelig angiver i dette høringssvar, så ønsker vi ikke, at afdøde personer omfattes af databeskyttelsesloven.

Skulle man i givet fald af eks. førnævnte årsag ønske en særlig beskyttelse, er det vores anbefaling og forslag:

- at man i givet fald indskriver dette specifikt ved, at afdødes personoplysninger er ikke omfattet af lovgivningen dog *undtaget særlige beskyttelsesforhold*.

Forslag til passus om særlige beskyttelsesforhold:

- *Særlige beskyttelsesforhold* er oplysninger om helbredsforhold, politisk overbevisning og strafbare forhold, idet disse kan fastsættes af den respektive ministers forhandling med justitsministeren til mere end eller mindre end en periode på 10 år.

Lovforslaget side 161:

Vi er dermed IKKE enig i Justitsministeriets vurdering at hensynet til afdødes eftermæle og nulevende pårørende alene skal begrunde, at oplysninger om den afdøde i en vis periode skal være omfattet af særlig beskyttelse ud fra en generel betragtning, men mener at det bør nærmere specificeres hvori denne beskyttelse ligger, ligesom den generelle periode på 10 år giver associationer til tidligere tiders østeuropæiske regimer / lukning af krigsarkiver o.lign.

Brancheforeningen skal på det kraftigste appellere til og anbefale, at man i Danmark følger EU-forordningens ordlyd uden en særlig dansk fortolkning og <u>dermed medtager følgende ordlyd</u> i den danske databeskyttelseslov:

<u>Afdøde personers personoplysninger er ikke omfattet af lovgivningen.</u>

Vi står selvfølgelig til rådighed for uddybning af vores høringssvar og deltager gerne i evt. møde herom, ligesom vi forventer at blive holdt ajour med nye / ændrede tiltag på området i relation til især håndtering af begravelser og dødsfald.

Med venlig hilsen

På Brancheforeningens vegne

Ole Roed Jakobsen

Branchedirektør

Mail: orj@bedemand.dk

Direkte tlf.: 3084 2001

DANSKE MEDIER

Pressens Hus
Skindergade 7
DK-1159 København K

Telefon 3397 4000

info@danskemedier.dk
www.danskemedier.dk

Justitsministeriet
Att.: Databeskyttelseskontoret
Slotsholmsgade 10
1216 København K

Sendt pr. e-mail til databeskyttelseskontoret@jm.dk

22. august 2017

Høringssvar vedr. udkast til forslag til databeskyttelseslov

Danske Medier har med tak modtaget Justitsministeriets høring over forslag til databeskyttelseslov.

Foreningen ser med tilfredshed på, at Justitsministeriet lægger op til, at der vedtages en generel lov (databeskyttelsesloven), som supplerer og præciserer reglerne i databeskyttelsesforordningen, inden for rammerne af denne forordning. Foreningen finder det særligt positivt, at lovforslaget på centrale områder er en videreførelse af de gældende regler i den nugældende persondatalov.

Danske Medier kan således helt overordnet tilslutte sig Justitsministeriets forslag til en supplerende databeskyttelseslov, men ønsker dog at fremkomme med enkelte bemærkninger.

Undtagelsesregler for mediernes behandling af personoplysninger (§ 3)

Danske Medier noterer med tilfredshed, at Justitsministeriet med § 3, stk. 4-8, lægger op til, at den gældende ordning vedrørende mediernes behandling af personoplysninger videreføres i videst muligt omfang. Det er afgørende for mediernes virke, at disse har adgang til at indsamle, bearbejde, offentliggøre og opbevare personoplysninger som led i deres redaktionelle virksomhed uden at være underlagt hovedparten af databeskyttelsesforordningens bestemmelser. Det er foreningens opfattelse, at de nuværende regler muliggør dette på passende vis.

Derfor blev Danske Medier også overrasket over, at det i bemærkningerne til lovforslagets enkelte bestemmelser, i forhold til § 3 på side 258, fremgår, at *"Det bemærkes i den forbindelse, at forordningens kapitel III vil finde anvendelse"*. Dette ville ikke være en videreførelse af den gældende ordning, men derimod en markant ændring af gældende ret.

På forespørgsel har Nanna Due Binø fra Justitsministeriet dog oplyst, at der er tale om en slåfejl, og at den korrekte henvisning skal være til forordningens kapitel VIII. Danske Medier konstaterer således, at der ikke er tilsigtet en ændring i retstilstanden.

Aldersgrænse for samtykke ved udbud af informationstjenester til børn (§ 6, stk. 2.)

Danske Medier konstaterer med tilfredshed, at Justitsministeriet har fulgt foreningens anbefaling om at gøre brug af undtagelsesreglen i databeskyttelsesforordningens artikel 6, stk. 1, sidste pkt. Det er foreningens opfattelse, at danske børn og unge er velorienterede om brugen af internettet og betydningen heraf, hvorfor det kan forsvares, at et barn på 13 år kan afgive samtykke til behandling af personoplysninger i forbindelse med brug af informationssamfundstjenester.

Foreningen står naturligvis til rådighed, såfremt ovenstående bemærkninger ønskes uddybet. Henvendelser herom kan rettes til undertegnede på e-mail rrb@danskemedier.dk eller telefon 3397 4000.

Med venlig hilsen
Danske Medier

Rasmus Roed Borg
Konsulent, cand.jur.

Danske Professionshøjskoler
University Colleges Denmark

J.NR.: 2015-0073/145798
Ref.: AE
aes@uc-dk.dk
+45 33 38 22 00
11. august 2017

Justitsministeriet

Att:databeskyttelseskontoret@jm.dk

Høringssvar: Over udkast til forslag til databeskyttelseslov

Danske Professionshøjskoler takker for invitationen som høringspart i høring om udkast til forslag til databeskyttelseslov. Med svarfrist 22. august 2017.

Vi har følgende bemærkninger.

Det hilses velkomment, at der ikke med lovforslaget sker indskrænkninger i forhold til de muligheder, som dataansvarlige i dag har for at foretage undersøgelser i statistisk eller videnskabeligt øjemed (forskning), jf. bemærkningerne til lovforslagets § 10.

Det bemærkes samtidig, at følgende formulering vedr. Datatilsynets tilladelse til videregivelse af personoplysninger som led i forskning efter Danske Professionshøjskolers opfattelse kan give anledning til uklarhed: "*Tilladelsen vil f.eks. kunne gives i forbindelse med anmeldelsen af en behandling, hvis den dataansvarlige allerede på anmeldelsestidspunktet kan forudse, at en videregivelse…..*" [Lovforslagets bemærkninger, side 271, 2. afsnit].

Danske Professionshøjskolers forstår lovforslaget og forordningen sådan, at den nuværende pligt til anmeldelse af forskningsprojekter (fællesanmeldelse) til Datatilsynet bortfalder. Citatets eksempel vedr. anmeldelse af en behandling kan således efter Danske Professionshøjskolers opfattelse give anledning til tvivl.

Det hilses ligeledes velkomment, at man med lovforslagets § 12 indfører en supplerende hjemmelsbestemmelse med henblik på at sikre, at offentlige arbejdsgivere fortsat kan behandle personoplysninger før, under og efter ansættelsesforhold i samme omfang som hidtil, herunder såvel følsomme som almindelige personoplysninger.

Herudover er der ikke yderligere bemærkninger til høringen.

Med venlig hilsen

Inge Friis Svendsen

d

Justitsministeriet
jm@jm.dk

24-08-2017
EMN-2017-03455
1074617
Katrine Stokholm

Høringsbrev om databeskyttelsesloven

Justitsministeriet har sendt udkast til databeskyttelseslov i høring med frist den 22. august 2017. Danske Regioner fremsender hermed sit høringssvar på baggrund af drøftelse af databeskyttelsesloven i Danske Regioners bestyrelse den 24. august 2017.

Danske Regioner finder overordnet, at EU-forordningen om persondatabeskyttelse sammen med databeskyttelsesloven udgør en god ramme om fremtidig behandling af personoplysninger. Danske Regioner finder det i den forbindelse positivt, at der i højere grad end hidtil skal anlægges en risikobaseret tilgang til persondata, hvor det bliver op til de dataansvarlige at gennemføre en konkret vurdering af, om behandling af persondata er i overensstemmelse med forordningen.

Patientbehandlingen har udviklet sig væsentligt siden den gældende persondatalovs vedtagelse. På moderne hospitaler foregår forskning og kvalitetsudvikling således parallelt med den aktuelle behandling af patienter. Samtidig foregår behandlingen af patienterne andre steder end på hospitalerne, nemlig hjemme hos den enkelte patient, i den kommunale hjemmepleje og hos den praktiserende læge. Danske Regioner finder det på den baggrund positivt, at forslaget lægger op til en fremtidssikret regulering af persondata, hvor der fokuseres på formål med den konkrete behandling afvejet med hensynet til persondatabeskyttelse.

Danske Regioner kan blandt andet støtte, at forslaget giver hjemmel til, at offentlige myndigheder fortsat kan have adgang til data, der understøtter deres opgaveløsning. Dette er særligt vigtigt på sundhedsområdet, hvor adgang til relevante persondata sikrer den bedst mulige patientbehandling.

DANSKE REGIONER
DAMPFÆRGEVEJ 22
2100 KØBENHAVN Ø
+45 35 29 81 00
REGIONER@REGIONER.DK
REGIONER.DK

Danske Regioner støtter, at der fastsættes en særlig bestemmelse om formålsbestemthed, hvorefter en minister efter forhandling med justitsministeren kan fastsætte nærmere regler om, at personoplysninger af offentlige myndigheder må viderebehandles til andre formål, end de oprindeligt var indsamlet til, uafhængigt af formålenes forenelighed.

Danske Regioner anerkender, at det er vanskeligt fuldstændigt at forudse behovet for at kunne behandle personoplysninger omfattet af forordningens artikel 9. Det kan derfor støttes, at der indsættes en bemyndigelse til, at vedkommende minister inden for forordningens rammer kan fastsætte yderligere regler om behandling af personoplysninger.

Danske Regioner støtter endvidere, at forordningen finder anvendelse på afdøde personers data og derved sikrer, at afdøde også har privatlivsbeskyttelse. Af hensyn til forskning og statistik er det dog afgørende, at der som foreslået er hjemmel til behandling af afdødes data inden for forordningens rammer.

Danske Regioner finder, at den nuværende persondatalovs § 10 skaber en fornuftig balance mellem hensynet til forskning og statistik og hensynet til beskyttelsen af den enkeltes privatliv. Det er derfor positivt, at denne balance også afspejles i forslaget til databeskyttelseslov. Endvidere noterer Danske Regioner sig, at det ikke er hensigten at etablere indskrænkninger i forhold til den gældende persondatalov.

Danske Regioner støtter, at det i § 10, stk. 4, foreslås at bemyndige sundhedsministeren til efter forhandling med justitsministeren at fastsætte regler om, at oplysninger, der er indsamlet til brug for forskning og statistik, senere kan bruges til andre formål, hvis behandlingen er nødvendig af hensyn til varetagelse af den registreredes vitale interesse. Dette er blandt andet relevant, hvis det i et forskningsprojekt viser sig, at en patient lider af alvorlig sygdom, der kan behandles. Det er endvidere relevant, hvis oplysninger indsamlet til forskning kan bruges som beslutningsgrundlag for aktuel behandling af patienten. Bestemmelsen bør udmøntes på en måde, der bedst muligt varetager patienternes interesse.

Det er uklart, hvorvidt det følger af § 6, stk. 3, at der skal foreligge et samtykke fra begge forældremyndighedsindehavere, såfremt forældremyndigheden er delt. Dette bør præciseres nærmere, eftersom forældre med fælles forældremyndighed, jf. forældreansvarsloven skal træffe beslutninger om barnet i fællesskab.

Danske Regioner noterer sig, at Databeskyttelsesforordningens artikel 9, stk. 2, litra b, g, h, i og j, ikke vil kunne anvendes som direkte behandlingshjemmel, og at disse bestemmelser derfor er udtryk for et nationalt råderum. Danske Regioner støtter, at artikel 9, stk. 2, litra b, g og h, foreslås "aktiveret" i persondatalovens § 7, stk. 2-4. Danske Regioner noterer sig i den forbindelse blandt andet, at muligheden i den nuværende persondatalov for at behandle oplysninger med henblik på at overholde den registreredes eller den dataansvarliges arbejdsretlige forpligtelser og specifikke rettigheder opretholdes.

Danske Regioner henstiller til, at artikel 9, stk. 2, litra i og j, tillige "aktiveres" i national ret under hensyn til behovet for at bruge data til at udvikle og drive velfærdsydelser. Her er der behov for en konkret vurdering af, hvilke hjemler der er behov for. Det er i den forbindelse væsentligt, at der foretages en risikovurdering, der afvejes mod behovet for at behandle data til gavn for den enkelte eller samfundet som helhed. Danske Regioner bidrager gerne til dette arbejde. Danske Regioner noterer sig, at den såkaldte "krigsregel" bortfalder, og at det fremover skal vurderes konkret, om IT-systemer skal opbevares inden for landets grænser af hensyn til statens sikkerhed.

Danske Regioner har desuden noteret sig, at spørgsmålet om sanktioner til offentlige myndigheder udestår. Danske Regioner forventer, at spørgsmålet om sanktioner sendes i høring og forbeholder sig ret til i den forbindelse at fremsende konkrete bemærkninger herom.

På en række områder er der behov for detaljerede vejledninger om, hvordan forordningen skal implementeres. Danske Regioner har noteret sig Justitsministeriets plan for vejledninger og bidrager gerne til arbejdet. Heri bør det blandt andet beskrives, hvordan der kan hentes inspiration i den gældende sikkerhedsbekendtgørelse og hvilke foranstaltninger, den dataansvarlige skal iværksætte.

For tekstnære kommentarer henvises til vedlagte notat herom.

Danske Regioner tager forbehold for de økonomiske konsekvenser af databeskyttelsesloven og EU-forordningen i regionerne.

Venlig hilsen

Bent Hansen

Stephanie Lose

NOTAT

23-08-2017
EMN-2017-03455
1078205
Katrine Stokholm

Tekstnære bemærkninger til forslaget til databeskyttelseslov

Udkastet til lovforslag til databeskyttelsesloven supplerer forordningen, der har virkning den 25. maj 2018. Det er Danske Regioners opfattelse, at lovforslaget samler fornuftigt op på områder, som forordningen ikke omhandler, men som de nationale stater har mulighed for at lovgive om.

Der er for databeskyttelsesforordningen udfærdiget en oversigt over vejledninger og tidsplan for offentliggørelse. På det arbejdsretlige område vil det ligeledes være hensigtsmæssigt, at der udarbejdes en vejledning, der redegør for og uddyber de særlige emner og problemstillinger, der ikke er behandlet i de øvrige vejledninger og som gør sig gældende inden for arbejdsret. På det regionale område gennemføres der overenskomstforhandlinger i 2018, og det vil derfor være nyttigt, såfremt en vejledning kan udarbejdes forinden. Danske Regioner deltager gerne med at bidrage til at udarbejde vejledning på området.

Danske Regioner noterer sig, at anmeldelsesordningen ikke er omfattet af høringsforslaget. Der skal derfor tages forbehold for, hvad denne anmeldelsesopgave erstattes af og hvordan, herunder de økonomiske konsekvenser for regionerne.

Specifikke bemærkninger

§ 10, stk. 3

Regionerne er af Datatilsynet blevet bemyndiget til selv at godkende videregivelse af data efter den gældende persondatalov § 10, stk. 3. Bemyndigelsen er begrænset til videregivelse af data inden for Danmarks grænser, og for biologisk materiale er bemyndigelsen begrænset til inden for den enkelte region. Det er uklart, om denne bemyndigelse fastholdes i uændret form. Der er behov for en afklaring heraf.

Danske Regioner finder, at Datatilsynets praksis om videregivelse af oplysninger til dataansvarlige i tredjelande bør understøtte og fremme forskning i Danmark inden for forordningens rammer.

§ 10, stk. 4

Danske Regioner noterer sig, at der med det nye stk. 4 gives bedre muligheder for anvendelse af forskningsresultater. Danske Regioner forventer at blive inddraget i det fremtidige lovforberedende arbejde ift. udarbejdelse af nye bestemmelser på det givne område.

Justitsministeriet
databeskyttelseskontoret@jm.dk

VI HJÆLPER HINANDEN

DANSKE SENIORER
Griffenfeldsgade 58
2200 København N
Tlf.: 3537 2422
Fax: 3535 2880
CVR: 10 78 87 14

Arbejdernes Landsbank
Kontonr.: 5301 0273256

info@danske-seniorer.dk
www.danske-seniorer.dk

Kontoret i Sdr. Omme:
Stadion Allé 11
7260 Sdr. Omme
Tlf.: 7534 1217
anj@danske-seniorer.dk

København N, den 22. august 2017

Høring over udkast til forslag til databeskyttelsesloven

Justitsministeriet har i skrivelse af 7. juli 2017 anmodet om eventuelle kommentarer til ovenstående lovforslag.

Lovforslaget er udformet som et supplement til en omfattende EU-forordning om beskyttelse af personoplysninger. Det giver ikke megen mening at kommentere forordningen, der er vedtaget; men der er trods alt overladt lidt til dansk lovgivning, så længe det ikke strider mod forordningen.

Danske Seniorer har især interesseret sig for anvendelse af sundhedsdata. Her skal patienten som hovedregel give tilladelse til, at data om vedkommende fra en del af sundhedsvæsenet anvendes i en anden del af sundhedsvæsenet. Hvad de færreste borgere ved er, at deres data uden deres samtykke og uden at de kan protestere bruges årligt i flere hundrede forskningsprojekter med anvendelse af cpr-numre.

Der sker ikke med det foreliggende lovforslag nogen ændring i bestemmelserne på dette område. Danske Seniorer finder imidlertid, at en borger skal kunne nægte at vedkommendes data anvendes til andet end det, de er givet for, eller at anvendelse kun må ske i egentlig anonymiseret form, det vil typisk sige kun ved anvendelse af fødselsdata plus køn. En sådan tilkendegivelse bør respekteres, uanset det kan gå ud over nogle ph.d. afhandlinger eller andre forskningsprojekter.

I lovforslagets § 2, stk. 5 står: "Loven om databeskyttelse finder anvendelse på afdøde personer i 10 år efter vedkommendes død." I stk. 6 står så at denne regel kan fraviges i begge retninger. Det anføres hverken i loven eller i bemærkningerne, hvilke kriterier der skal lægges til grund for at fravige i den ene eller anden retning.

Danske Seniorer har ved telefonisk henvendelse til Justitsministeriet forsøgt at få oplyst, hvilke retsregler, der gælder, når databeskyttelsesloven ikke længere gælder. Sagsbehandleren i ministeriet kunne ikke svare herpå. Er der som hovedregel efter 10 år fri adgang til en afdød persons sundhedsdata? Hvis det er tilfældet, forekommer 10 år at være et alt for kort tidsrum. I den udstrækning man ønsker at fravige hovedreglen, bør der endvidere være generelle kriterier, der er kendt af offentligheden.

Med venlig hilsen

Jørgen Fischer
Landsformand

Henrik Grüber Sivgaard
Direktør

DATATILSYNET

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendt til: databeskyttelseskontoret@jm.dk og
jm@jm.dk

22. august 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. 2017-111-0133
Dok.nr. 439245
Sagsbehandler
Signe Vestergård
Abildskov
Direkte 3319 3212

Vedrørende høring over udkast til forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) – Justitsministeriets sagsnr.: 2016-7910-0021

Ved e-mail af 7. juli 2017 har Justitsministeriet anmodet Datatilsynet om eventuelle bemærkninger til ovennævnte lovforslag.

Datatilsynet skal – efter at sagen har været behandlet i Datarådet - udtale følgende:

1. Indledning

Datatilsynet hilser de nye regler på databeskyttelsesområdet velkommen. Reglerne vil efter tilsynets opfattelse styrke beskyttelsen af borgernes personlige oplysninger.

Datatilsynet har i den forbindelse navnlig noteret sig den styrkelse, der følger af forordningens bestemmelser om databeskyttelsesrådgivere, fortegnelser over behandlingsaktiviteter, dokumentationskrav og konsekvensanalyser og sikkerhedsbrud samt bestemmelserne om databeskyttelse gennem design og standardindstillinger. Det er Datatilsynets håb og forventning, at de nye krav sammen med mulighederne for betydelig strengere sanktioner ved overtrædelse af lovgivningen vil bidrage til at skabe større opmærksomhed omkring hensynet til persondatabeskyttelse og dermed medføre en mærkbar forbedring af beskyttelsen.

Datatilsynet er enig med Justitsministeriet i, at det er nødvendigt i tilknytning til databeskyttelsesforordningen at gennemføre en særskilt lov som supplement til forordningen.

I forhold til udkastet til lovforslag har Datatilsynet følgende bemærkninger:

2. Lovforslagets enkelte bestemmelser

Ad § 1

Datatilsynet foreslår, at der i sidste punktum i *stk. 2* tilføjes "og § 3 i denne lov".

Ad § 2

Der henvises i *stk. 1* til "databeskyttelsesforordningens artikel 5, stk. 1-3". Det samme gør sig gældende i bemærkningerne til bestemmelsen, hvor der således også henvises til artikel 5, stk. 1-3.

Datatilsynet bemærker, at artikel 5 i forordningen kun består af to stykker.

Datatilsynet skal endvidere foreslå, at der i *stk. 5 og stk. 6* inden ordet "afdøde" indsættes "oplysninger om".

Ad § 3

Datatilsynet har noteret sig, at bestemmelserne i *stk. 4-6* er en videreførelse af gældende ret. Det er tilsynets opfattelse, at disse regler – og deres sammenhæng med lov om massemediers informationsdatabaser – er uhensigtsmæssige og unødigt komplicerede. Datatilsynet skal derfor opfordre til, at der snarest foretages en revision af hele regelsættet.

Ad § 5

Datatilsynet foreslår, at *stk. 3, sidste pkt.*, affattes således:

"1. pkt. finder ikke anvendelse på behandling af oplysninger i medfør af § 10."

Ad § 7

Der henvises til pkt. 4 nedenfor om anmeldelsespligt og tilladelseskrav.

Ad § 9

Der henvises til pkt. 4 nedenfor om anmeldelsespligt og tilladelseskrav.

Ad § 10

Spørgsmålet om fastsættelse af regler om behandling af oplysninger i forbindelse med statistiske eller videnskabelige undersøgelser til erstatning for eller videreførelse af § 10 i persondataloven har kun i meget begrænset omfang været berørt i forbindelse med tilblivelsen af betænkningen og lovforslaget.

Datatilsynet har på den baggrund gjort sig særlige overvejelser om dette emne.

Datatilsynet foreslår, at bestemmelsen i § 10 formuleres således:

> **§ 10**. Oplysninger som nævnt i databeskyttelsesforordningens artikel 9, stk. 1, og artikel 10 må behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig af hensyn til udførelsen af undersøgelserne.
>
> *Stk. 2*. Oplysninger, der er behandlet i medfør af stk. 1, må ikke senere behandles i andet end videnskabeligt eller statistisk øjemed. Det samme gælder behandling af andre oplysninger, som alene foretages i statistisk eller videnskabeligt øjemed i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra e, første led, eller litra f.
>
> *Stk. 3*. De af stk. 1 og 2 omfattede oplysninger må kun videregives til behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde, jf. forordningens artikel 3, efter forudgående tilladelse fra tilsynsmyndigheden. Der kræves ligeledes tilladelse fra tilsynsmyndigheden til videregivelse af biologisk materiale.
>
> *Stk. 4.* Tilsynsmyndigheden kan fastsætte generelle vilkår for videregivelsen af oplysninger omfattet af stk. 1 og 2, herunder for videregivelser, der ikke kræver tilladelse efter stk. 3.
>
> *Stk. 5.* Stk. 2-4 finder ikke anvendelse, hvis den registrerede har givet sit udtrykkelige samtykke til den senere behandling, eller hvis oplysningerne siden indsamlingen tydeligvis er offentliggjort af den registrerede selv.
>
> *Stk. 6*. Vedkommende minister kan efter forhandling med justitsministeren uanset stk. 2 fastsætte regler om, at oplysninger omfattet af stk. 1 og 2, som er behandlet med henblik på at udføre videnskabelige undersøgelser, senere kan behandles i andet end statistisk eller videnskabeligt øjemed, hvis behandlingen er nødvendig af hensyn til varetagelse af den registreredes vitale interesser.

Ad stk. 1

Datatilsynet foreslår, at det følgende indsættes i bemærkningerne til lovforslagets § 10 under andet afsnit om bestemmelsens stk. 1:

> ”Behandlingen bliver ikke omfattet af § 10, i det omfang indsamlingen af oplysningerne sker på grundlag af den registreredes udtrykkelige samtykke, eller hvor der er tale om oplysninger, der tydeligvis er offentliggjort af den registrerede selv. Der er således også fortsat valgfrihed for den dataansvarlige i forhold til at vælge mellem samtykke og § 10, stk. 1, som hjemmelsgrundlag. Det bemærkes herved, at samtykke ikke altid er en hensigtsmæssig behandlingshjemmel, da samtykket kan tilbagekaldes af den registrerede, jf. forordningens artikel 7, stk. 3.”

Ad stk. 2

For så vidt angår bemærkningerne til lovforslagets § 10, stk. 2, foreslår Datatilsynet, at afsnittet formuleres således:

> ”Det følger af stk. 2, at der ikke senere må ske behandling, herunder videregivelse, af oplysninger, som er behandlet i medfør af stk. 1, til andre formål. Dette medfører bl.a., at oplysningerne ikke må anvendes til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer. Tilsvarende gælder med hensyn til behandling af andre oplysninger, som i henhold til artikel 6,

> stk. 1, litra e, første led, eller litra f alene foretages med henblik på at udføre statistiske eller videnskabelige undersøgelser.
>
> Der vil således alene kunne ske efterfølgende behandling, herunder videregivelse, i andet end videnskabelig eller statistisk øjemed efter stk. 5 og 6."

Datatilsynet skal i den forbindelse bemærke, at hvis henvisningen i det foreliggende udkast til lovforslag skal forstås således, at formålsbegrænsningen gælder generelt for artikel 6-oplysninger, vil det indebære en mere restriktiv adgang til at behandle ikke-følsomme oplysninger end følsomme oplysninger. Det bemærkes i den forbindelse, at der efter § 10, stk. 1, er valgfrihed for den dataansvarlige i forhold til at vælge mellem samtykke og § 10, stk. 1, som hjemmelsgrundlag til behandling af følsomme oplysninger, jf. herved det anførte ovenfor i Datatilsynets forslag til bemærkninger til lovforslagets § 10, stk. 1.

Formålsbegrænsningen i stk. 1 og 2 indebærer, at personoplysninger, som er behandlet i medfør af § 10, ikke kan videregives med henblik på andet end at udføre statistiske eller videnskabelige undersøgelser, selvom oplysningerne videregives i en form, der ikke umiddelbart er personhenførbar for modtageren. Som konsekvens heraf kan oplysninger omfattet af § 10 efter Datatilsynets forståelse heller ikke indgå i materiale, der publiceres i videnskabelige tidsskrifter, medmindre oplysningerne anonymiseres i en sådan grad, at de bringes helt uden for persondatalovens anvendelsesområde, hvilket i nogle tilfælde ikke er praktisk muligt uden samtidig at give køb på formålet med offentliggørelsen.

Datatilsynet skal i den forbindelse pege på, at det kan overvejes at lempe reglerne, så oplysninger, som behandles i medfør af lovforslagets § 10, f.eks. kan indgå i materiale, der publiceres i "anerkendte" videnskabelige tidsskrifter mv., hvis oplysningerne forinden offentliggørelsen som minimum pseudonymiseres i en grad, der svarer til det, der gælder på forvaltningslovens og offentlighedslovens område.

Ad stk. 3 og 4

Datatilsynet skal bemærke, at tilsynet som udgangspunkt ikke har forudsætninger for at tilsidesætte den dataansvarliges vurdering af, at modtagerundersøgelsen er af væsentlig samfundsmæssig betydning, ligesom tilsynet normalt kun på et overordnet niveau kan vurdere, om (alle) de oplysninger, der ønskes videregivet, er nødvendige for modtagerens undersøgelse.

Datatilsynets sagsbehandling i relation til tilladelseskravet i forbindelse med videregivelse til tredjemand består således primært i at sikre, at oplysningerne udelukkende videreanvendes til videnskabelige eller statistiske undersøgelser. På den baggrund stiller Datatilsynet normalt vilkår om pseudonymisering, når oplysninger skal videregives til EU-/EØS-lande, og der gives som altovervejende udgangspunkt ikke tilladelse til videregivelse til dataansvarlige i (usikre) tredjelande.

Datatilsynet indførte i 2015 en ordning, hvorefter offentlige myndigheder blev meddelt generelle videregivelsestilladelser med vilkår om bl.a. førelse af interne "fortegnelser" over de foretagne videregivelser. Datatilsynet har imidlertid fastholdt, at myndighederne skal søge individuelle tilladelser, når der er tale om videregivelse til dataansvarlige i udlandet eller videregivelse af biologisk materiale fra biobanker (der anses som manuelle registre).

Hvis Datatilsynet fortsat skal være tilladelsesmyndighed efter stk. 3, foreslås det – i forlængelse af den ordning, der allerede er indført for offentlige myndigheder – generelt at begrænse tilladelseskravet til de tilfælde, hvor der er tale om biologisk materiale, og de tilfælde, hvor oplysningerne skal videregives ud af forordningens territoriale anvendelsesområde. Det kan i den forbindelse overvejes at bemyndige Datatilsynet til også at fastsætte vilkår for de videregivelser, der ikke længere måtte kræve tilladelse, i form af generelle vilkår, der offentliggøres.

Til brug for Datatilsynets vurdering af modtagne ansøgninger om videregivelsestilladelser kan det overvejes at indføre en ordning, hvorefter de dataansvarlige forskningsinstitutioner mv., der behandler oplysninger i videnskabelige eller historiske forskningsformål eller til statistiske formål, forpligtes til at offentliggøre de fortegnelser, som skal føres i medfør af forordningens artikel 30. En sådan ordning vil smidiggøre sagsoplysningen for såvel ansøgerne som Datatilsynet og vil samtidig kunne bidrage til en generel åbenhed om behandlingerne.

Hvis der ønskes en egentlig sagkyndig myndighedsvurdering i forbindelse med en tilladelsesordning, kan det for så vidt angår videregivelse til og fra sundhedsvidenskabelig forskning overvejes i stedet at lægge opgaven i f.eks. regi af det videnskabsetiske komitésystem. Det bemærkes herved, at langt størstedelen af de ansøgninger, som Datatilsynet modtager efter stk. 3, angår sundhedsvidenskabelig forskning.

Det fremgår af bemærkningerne til § 10, stk. 3, i udkastet til lovforslag, at en tilladelse efter § 10, stk. 3, f.eks. vil kunne gives i forbindelse med anmeldelsen af en behandling, hvis den dataansvarlige allerede på anmeldelsestidspunktet kan forudse, at en videregivelse til tredjeland til brug for statistiske eller videnskabelige undersøgelser vil blive aktuelt.

Der ses imidlertid ikke med lovforslaget at blive videreført en anmeldelsespligt eller en pligt til at indhente tilladelse til behandling af følsomme oplysninger, der alene sker med henblik på at udføre statistiske og videnskabelige undersøgelser af væsentlig samfundsmæssig interesse. Datatilsynet kan tilslutte sig, at der ikke længere skal være en sådan anmeldelsespligt.

Datatilsynet foreslår på den baggrund, at bemærkningerne i udkastet til § 10, stk. 3 erstattes med følgende:

> "Bestemmelsen i stk. 3 fastsætter, at videregivelse til behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde, jf. forordningens

> artikel 3, kun kan ske efter forudgående tilladelse fra vedkommende tilsynsmyndighed. Det samme gælder for videregivelse af biologisk materiale.
>
> Det medfører bl.a., at videregivelse af oplysninger til behandling, som foretages af en dataansvarlig eller en databehandler, der er etableret i et tredjeland, hvor der ikke er tale om behandlingsaktiviteter som nævnt i forordningens artikel 3, stk. 2, litra a og b, eller en behandling som nævnt i forordningens artikel 3, stk. 3, kun kan ske efter forudgående tilladelse fra vedkommende tilsynsmyndighed. Videregivelse af biologisk materiale til tredjemand kan ligeledes kun ske efter forudgående tilladelse fra vedkommende tilsynsmyndighed. Videregivelse kan i givet fald kun ske med henblik på behandlinger til videnskabelige eller statistiske formål.
>
> Ved videregivelse af oplysninger til tredjemand til behandling inden for databeskyttelsesforordningens territoriale anvendelsesområde, herunder videregivelser til dataansvarlige, der er etableret i Danmark eller andre EU-lande, skal der derimod ikke indhentes en tilladelse fra vedkommende tilsynsmyndighed, medmindre der er tale om videregivelse af biologisk materiale. Vedkommende tilsynsmyndighed kan imidlertid efter § 10, stk. 4, fastsætte generelle vilkår for disse videregivelser."

Ad stk. 5

Formålsbegrænsningen i persondatalovens § 10, stk. 2, gælder, uanset om den registrerede måtte samtykke til viderebehandling til andre formål. Det er imidlertid vanskeligt at se beskyttelseshensynet i den sammenhæng, idet oplysningerne under alle omstændigheder lovligt ville kunne genindsamles med samtykke inden for rammerne af de grundlæggende principper i artikel 5. Hensynet til de registreredes selvbestemmelse taler ligeledes imod at opretholde en sådan begrænsning.

På den baggrund foreslår Datatilsynet, at § 10, stk. 5, som fremgår ovenfor, indsættes i bestemmelsen.

Datatilsynet foreslår endvidere, at følgende bemærkninger til stk. 5 indsættes i bemærkningerne til § 10:

> "Det følger af bestemmelsen, at § 10, stk. 2-4 ikke finder anvendelse, hvis den registrerede har givet sit udtrykkelige samtykke til den senere behandling, eller hvis oplysningerne siden indsamlingen tydeligvis er offentliggjort af den registrerede selv.
>
> Det medfører, at den registrerede kan give sit udtrykkelige samtykke til, at oplysninger, der er behandlet i medfør af § 10, stk. 1, må behandles i andet end statistisk eller videnskabeligt øjemed. En sådan situation er at sidestille med en fornyet indsamling af de pågældende oplysninger.
>
> Den registrerede kan endvidere efter den foreslåede bestemmelse give samtykke til, at de af stk. 1 og 2 omfattede oplysninger kan videregives til behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde, samt give samtykke til, at biologisk materiale som behandles efter § 10, stk. 1, kan videregives til tredjemand.
>
> Bestemmelsen medfører endvidere, at hvis oplysningerne siden indsamlingen tydeligvis er offentliggjort af den registrerede selv, kan oplysningerne behandles i andet end statistisk eller videnskabeligt øjemed samt videregives til

> behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde.
>
> Det bemærkes i den forbindelse, at et samtykke skal leve op til betingelserne i databeskyttelsesforordningens artikel 4, nr. 11, og artikel 7.
>
> Ved viderebehandling i andet end statistisk eller videnskabeligt øjemed på baggrund af, at den registrerede tydeligvis har offentliggjort oplysningerne, skal det i øvrigt overvejes, om der forud for en viderebehandling skal gives den registrerede oplysning om dette andet formål og andre relevante oplysninger, jf. artikel 13, stk. 3 og artikel 14, stk. 4
>
> Offentliggørelse i bestemmelsens forstand foreligger, hvis oplysningerne er bragt til kundskab hos en bredere kreds af personer. Dette vil f.eks. være tilfældet, hvis oplysningerne viderebringes gennem tv, aviser eller lignende landsdækkende medier. Også andre former for videregivelse af oplysninger vil kunne anses for offentliggørelse i bestemmelsens forstand. Det er en betingelse, at oplysningerne er offentliggjort på den registreredes foranledning. Oplysninger, som andre, f.eks. pressen, af egen drift har offentliggjort, er således ikke omfattet. ”

Ad stk. 6

En undtagelse på baggrund af den registreredes vitale interesser er ikke kun relevant på sundhedsområdet, og det bør derfor overvejes, om denne undtagelse i forhold til § 10, stk. 4, i udkastet til lovforslag skal udvides til at omfatte videnskabelig forskning generelt eller evt. til yderligere specifikke områder.

Datatilsynet har f.eks. modtaget henvendelser om, at der på baggrund af besvarelser i spørgeskemaundersøgelser er opstået mistanke om seksuelle overgreb mod børn. Sådanne henvendelser besvares normalt med vejledning om persondatalovens § 10 samt om betingelserne for nødret. Datatilsynet har ikke viden om, i hvilket omfang disse mistanker har holdt stik.

På den baggrund foreslår Datatilsynet, at første afsnit i bemærkningerne til lovforslagets § 10, stk. 4, (§ 10, stk. 6, ifølge Datatilsynets forslag) omformuleres til følgende ordlyd:

> ”Det foreslås i [….] at bemyndige vedkommende minister til efter forhandling med justitsministeren – og uanset udgangspunktet i stk. 2 – at fastsætte regler om, at oplysninger omfattet af stk. 1 og 2, som er behandlet med henblik på at udføre videnskabelige undersøgelser og statistik, senere kan behandles til andre formål end videnskabelige eller statistiske formål, hvis en sådan behandling er nødvendig til varetagelse af den registreredes vitale interesser. Bestemmelsen er tiltænkt et meget snævert anvendelsesområde. Ved videregivelse af oplysninger om helbredsmæssige forhold vil det være en forudsætning, at oplysningerne videregives gennem den patientansvarlige læge.”

Herudover foreslår Datatilsynet følgende afsnit indsat i bemærkningerne til bestemmelsen:

> ”Det er i øvrigt muligt med bemyndigelsesbestemmelsen at fastsætte regler, der tillader behandling af personoplysninger omfattet af stk. 1 og 2, på andre områder end sundhedsområdet.
>
> Det kan f.eks. tænkes at være nødvendigt af hensyn til varetagelse af den registreredes vitale interesser at behandle personoplysninger til andre formål end videnskabelige og statistiske formål, f.eks. i situationer, hvor der i forbindelse med en statistik eller videnskabelig undersøgelse opstår mistanke om seksuelle overgreb mod børn.”

Ad § 11

Datatilsynet kan af de grunde, som Justitsministeriet har anført i bemærkningerne, tilslutte sig indsættelsen af bestemmelsen i *stk. 2, nr. 4*, der indebærer, at private – i modsætning til i dag – bør have mulighed for at behandle oplysninger om personnummer, når betingelserne i forslagets § 7 er opfyldt.

Datatilsynet antager i øvrigt, at henvisningen til stk. 4 i bemærkningerne til bestemmelsen rettelig vedrører stk. 2, nr. 4 (og derfor bør placeres højere oppe i teksten). De to sidste afsnit i bemærkningerne forekommer overflødige og bør udgå.

Ad § 13

I *stk. 6* skal der i stedet for henvisning til stk. 4 henvises til stk. 5. Endvidere bør ”og denne lovs…” ændres til ”eller denne lovs…”.

Også i bemærkningerne til bestemmelsen er der fejlagtigt henvist til stk. 4.

Til det anførte i bemærkningerne vedrørende undersøgelse i CPR kan Datatilsynet supplerende oplyse, at en undersøgelse i CPR efter tilsynets praksis ikke kan ske ved brug af den såkaldte Robinsonliste, da denne kun opdateres kvartalsvis og ikke indeholder oplysninger om navne- og adressebeskyttelse. Undersøgelsen må derfor ske ved henvendelse til CPR med anmodning om udtræk efter reglerne i kap. 10 i lov om Det Centrale Personregister.

Ad § 19

Der henvises til pkt. 4 nedenfor om anmeldelsespligt og tilladelseskrav.

Ad § 22

I *stk. 4, 1. linje*, skal ordet ”i” slettes.

Ad § 26

Der henvises til pkt. 4 nedenfor om anmeldelsespligt og tilladelseskrav.

Ad § 27

Datatilsynet skal henstille, at formandsposten i Datarådet fortsat vil blive beklædt af en højesteretsdommer.

Ad § 33

Ordet "også" bør erstattes med "tilsvarende".

Efter Datatilsynets opfattelse forekommer det uklart, hvad der nærmere ligger i henvisningen til § 22. Den nærmere betydning heraf bør derfor efter tilsynets opfattelse uddybes eller eksemplificeres i bemærkningerne til bestemmelsen.

Datatilsynet foreslår på den baggrund, at det følgende indsættes i bemærkningerne til lovforslagets § 33:

> "Henvisningen til § 22 indebærer, at Datatilsynet er berettiget – og efter omstændighederne også forpligtet – til at undlade at offentliggøre oplysninger fra sager, som tilsynet har behandlet, hvis offentlighedens interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til private eller offentlige interesser."

Ad § 41

Vedrørende *stk. 4* bemærkes, at "pålægges" skal erstattes af "pålæg" eller "tildeling".

Datatilsynet har noteret sig, at stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder udestår.

Datatilsynet bemærker i den forbindelse, at der gennem tiden har været mange eksempler på, at offentlige myndigheder har begået gentagne overtrædelser af databeskyttelseslovgivningen, hvilket efter tilsynets opfattelse kunne tale for også at fastsætte bestemmelser om straf for offentlige myndigheder.

Det bemærkes i øvrigt, at det ikke fremgår af straffebestemmelserne i udkastet til lovforslag, at disse alene omfatter private.

Ad § 47

Bestemmelsen indebærer, at der ikke skal indhentes ny tilladelse til behandlinger, der også efter lovens ikrafttræden vil kræve en tilladelse fra tilsynsmyndigheden.

En sådan ordning vil imidlertid efter Datatilsynets opfattelse ikke være hensigtsmæssig, idet de eksisterende tilladelser – der ikke er tidsbegrænsede – vil indeholde henvisninger til en lovgivning, der efter den 25. maj 2018 ikke længere eksisterer.

Datatilsynet foreslår på den baggrund, at ordlyden af lovforslagets § 47 ændres til følgende:

> "Tilladelser, som Datatilsynet i dag har givet efter persondatalovens § 50, stk. 1, nr. 2-3, gælder, indtil de erstattes af en ny tilladelse efter lovforslagets § 7, stk. 4, § 19 eller § 26, stk. 1."

Formuleringen i afsnit 2.6.3.4., afsnit 2 (side 219) ændres tilsvarende.

Det kan i den forbindelse efter Datatilsynets opfattelse tillige overvejes at fastsætte en frist – på f.eks. ½ år – for indgivelse af ansøgning om ny tilladelse til erstatning for en tilladelse, der er meddelt i medfør af persondataloven.

3. De almindelige bemærkninger til lovforslaget

Ad afsnit 1.1., afsnit 11-14 (side 151-152)

I de nævnte afsnit er der henvist til en række bestemmelser i forordningen, hvorefter medlemsstaterne kan eller skal fastsætte nationale regler.

Datatilsynet bemærker, at der ikke ses at være tale om en udtømmende opregning af bestemmelser, hvorefter medlemsstaterne kan eller skal fastsætte nationale regler. Datatilsynet finder, at dette bør fremgå af teksten.

Ad afsnit 1.1., afsnit 15 (side 152)

Datatilsynet bemærker, at lovforslaget ikke alene – som forordningen – har til formål at beskytte fysiske personer, men også har til formål på visse områder at beskytte virksomheder.

Ad afsnit 1.2., afsnit 8 (side 153)

Datatilsynet finder, at sidste sætning i afsnittet bør udgå, idet dens betydning forekommer uklar.

Ad afsnit 2.1.1., afsnit 4 (side 156)

Datatilsynet foreslår, at følgende tilføjes sidst i afsnittet:

> "Justitsministeren kan i medfør af persondatalovens § 1, stk. 6, uden for de i stk. 4 nævnte tilfælde bestemme, at lovens regler helt eller delvis skal finde anvendelse på behandling af oplysninger om virksomheder mv., som udføres for private."

Ad afsnit 2.1.1., afsnit 5-7 (side 156)

Datatilsynet foreslår, at formuleringen i de nævnte afsnit ændres til følgende:

> "Persondataloven gælder endvidere ifølge lovens § 1, stk. 5, for offentlige myndigheders videregivelse til kreditoplysningsbureauer af oplysninger om

> virksomheder mv. angående gæld til det offentlige, hvis oplysningerne behandles helt eller delvis elektronisk eller er eller vil blive indeholdt i et register, jf. henvisningen til stk. 1 i bestemmelsen. Vedkommende minister kan i medfør af persondatalovens § 1, stk. 7, uden for de i stk. 5 nævnte tilfælde bestemme, at lovens regler helt eller delvis skal finde anvendelse på behandling af oplysninger om virksomheder mv., som udføres for den offentlige forvaltning."

Datatilsynet kan i den forbindelse henvise til side 27 i Betænkning om Databeskyttelsesforordningen[1].

Ad afsnit 2.1.2., afsnit 4 (side 158)

Datatilsynet foreslår, at afsnittet om, at forordningen også gælder for domstolene, udgår, da sætningen ikke indgår naturligt i sammenhængen.

Ad afsnit 2.1.3.2., første afsnit (side 160)

Datatilsynet skal til henvisningen til "persondatalovens § 1, stk. 2-7" bemærke, at bestemmelserne ikke alene regulerer ikke-elektronisk behandling af personoplysninger men også bl.a. behandling af oplysninger om virksomheder, jf. § 1, stk. 4-7.

Datatilsynet bemærker i øvrigt, at selv om virksomheder vil være omfattet at nogle af reglerne i lovforslaget og i forordningen, vil de rettigheder i forhold til behandling af sager på europæisk plan, som fremgår af forordningen, ikke finde anvendelse for virksomheder.

Ad afsnit 2.1.3.2., afsnit 6 (side 161)

Datatilsynet kan tilslutte sig forslaget om, at der indføres en begrænsning på 10 år efter vedkommendes død for så vidt angår behandling af oplysninger om afdøde.

Datatilsynet skal i den forbindelse henstille, at der i bemærkningerne til lovforslagets § 2, stk. 6, medtages eksempler på områder, hvor det må antages at være nødvendigt eller hensigtsmæssigt at fastsætte andre frister. Tilsynet skal i den forbindelse pege på, at det bl.a. inden for sundhedsområdet vil være relevant at lade personoplysninger være omfattet af lovgivningen i en (betydelig) længere periode end 10 år.

Ad afsnit 2.2.1., afsnit 4 (side 162)

Datatilsynet foreslår, at der efter det nævnte afsnit indsættes følgende afsnit:

> "Ved "tredjeland" forstås ifølge persondatalovens § 3, nr. 9, en stat, som ikke indgår i Det Europæiske Fællesskab (nu Den Europæiske Union), og som ikke har gennemført aftaler, der er indgået med Det Europæiske Fællesskab, og som indeholder regler svarende til direktiv 95/46/EF af 24. oktober 1995 om

[1] Betænkning nr. 1565 om Databeskyttelsesforordningen (2016/679) – og de retlige rammer

> beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger."

Ad afsnit 2.3.1.1., afsnit 3 side (165-166)

Datatilsynet foreslår, at følgende indsættes efter det nævnte afsnit:

> "Det følger af § 5, stk. 2, sidste pkt., at senere behandling af oplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, ikke anses for uforenelig med de formål, hvortil oplysningerne er indsamlet. Herved sikres det, at oplysninger, der ikke oprindelig er indsamlet med disse formål for øje, under alle omstændigheder vil kunne anvendes til senere behandling i historisk, statistisk eller videnskabeligt øjemed. En forudsætning herfor er dog, at den senere behandling alene sker til disse formål.
>
> Det bemærkes i den forbindelse, at det følger af persondatalovens § 10, stk. 2, at der ikke senere må ske behandling af oplysninger, som er omfattet af § 10, stk. 1, i andet end statistisk eller videnskabeligt øjemed. Det samme gælder behandling af andre oplysninger, som alene foretages i statistisk eller videnskabeligt øjemed, jf. stk. 6.
>
> Dette medfører bl.a., at oplysningerne ikke må anvendes til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer. Der vil således alene kunne ske efterfølgende behandling, herunder videregivelse, jf. stk. 3, til private forskere eller offentlige myndigheder i det omfang, behandlingen alene sker med henblik på udførelsen af andre statistiske eller videnskabelige undersøgelser. Tilsvarende gælder med hensyn til behandling af andre oplysninger, som i henhold til § 6 alene foretages med henblik på at udføre statistiske eller videnskabelige undersøgelser."

Ad afsnit 2.3.1.2., sidste afsnit (side 167)

Datatilsynet foreslår, at "i udgangspunktet" udgår fra den sidste sætning i afsnittet, da anvendelsen af "ikke-uforenelighedstesten" i alle tilfælde forudsætter, at der foretages en konkret vurdering.

Ad afsnit 2.3.2.3., afsnit 6 (side 173)

Datatilsynet har noteret sig forslaget om, at der fastsættes en aldersgrænse for børns samtykke til anvendelse af informationssamfundstjenester på 13 år.

Datatilsynet skal i den forbindelse understrege vigtigheden af, at datasikkerhed og beskyttelse af personoplysninger bliver en del af undervisningen i folkeskolen.

Datasikkerhed og beskyttelse af personoplysninger kan eventuelt tilføjes i § 7, stk. 1, i lov om folkeskolen[2] som et af de obligatoriske emner, der indgår i undervisningen i grundskolen på lige fod med færdselslære, sundheds- og seksualundervisning og familiekundskab samt uddannelse og job.

Ad afsnit 2.3.2.3., afsnit 28 (side 177)

[2] Lov nr. 747 af 20. juni 2016 om folkeskolen med senere ændringer.

Datatilsynet tilslutter sig Justitsministeriets bemærkning om, at det med lovforslaget fortsat er en forudsætning, at der skal ligge en særlig og klar lovhjemmel til grund for systematisk offentliggørelse af oplysninger om kontrolresultater og afgørelser mv. i ikke anonymiseret form. Datatilsynet henviser i den forbindelse til Betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. kapitel 4, pkt. 2.1.

Ad afsnit 2.3.3.3., afsnit 4 (side 183)

Datatilsynet bemærker, at det ikke fremgår klart af afsnittet, at det kun er i sidstnævnte tilfælde (væsentlig samfundsinteresse), at der efter forslaget skal indhentes tilladelse til behandlingen.

Datatilsynet foreslår på den baggrund, at de sidste to sætninger i afsnittet omformuleres til følgende:

> "Tilladelsesmyndigheden giver efter lovforslagets § 7, stk. 4, 2. pkt. tilladelse til behandling af følsomme oplysninger, som er nødvendig af hensyn til væsentlige samfundsinteresser, hvis behandlingen ikke foretages af eller for en offentlig myndighed. Der kan efter lovforslagets § 7, stk. 4, 3. pkt. fastsættes nærmere vilkår for behandlingen i en tilladelse efter lovforslagets 2. pkt."

Der henvises i øvrigt til det nedenfor under pkt. 4 anførte om anmeldelsespligt og tilladelseskrav.

Ad afsnit 2.3.3.3., afsnit 12 (side 184-185)

Datatilsynet bemærker, at der udover de foranstaltninger, der nævnes i afsnittet som en del af den dataansvarliges "værktøjskasse", også bør henvises til de foranstaltninger, der skal træffes i medfør af forordningens artikel 25.

Endvidere bemærkes, at en del af de omtalte foranstaltninger også er relevante ved behandling af almindelige ikke-følsomme oplysninger omfattet af artikel 6 og personoplysninger vedrørende straffedomme og lovovertrædelser omfattet af artikel 10.

Ad afsnit 2.3.10.3., afsnit 2 (side 200)

Datatilsynet er ikke klar over, hvad der menes med, at der lægges vægt på, at der ved udformningen af bestemmelsen i lovforslagets § 14 skabes klarhed om reglerne om arkivering af personoplysninger mv.

Datatilsynet bemærker i den forbindelse, at lovforslagets § 14 er identisk med § 14 i den gældende persondatalov, som ikke i sig selv indeholder regler om behandling eller arkivering af personoplysninger, men blot henviser til arkivlovgivningen.

Ad afsnit 2.3.11.1., afsnit 4 (side 201)

Datatilsynet foreslår, at ordet ”ofte” i 1. sætning erstattes med ”normalt”.

Ad afsnit 2.7.3.1., afsnit 2 (side 226)

Det fremgår af afsnittet, at Datatilsynet har tilsynskompetence på alle områder inden for dansk jurisdiktion omfattet af forordningen og lovforslaget (bortset fra behandling af oplysninger for domstolene), og at øvrige tilsyn ”såsom Finanstilsynet og Forbrugerombudsmanden, der ikke har status som uafhængige tilsynsmyndigheder, vil have karakter af supplerende tilsyn i forhold til Datatilsynets generelle tilsyn”.

Det står ikke Datatilsynet klart, hvad der menes med ”supplerende tilsyn”.

Datatilsynet kan i den forbindelse henvise til, at der under den nuværende retstilstand gennem årene jævnligt har været rejst spørgsmål om afgrænsningen af Datatilsynets kompetence i forhold til bl.a. Finanstilsynet og Forbrugerombudsmandens kompetence, og at der fortsat i nogle henseende må anses at være tvivl herom.

Datatilsynet skal derfor opfordre til, at det i bemærkningerne til lovforslaget nærmere præciseres, hvad der forstås ved ”supplerende tilsyn”, herunder om det indebærer, at Datatilsynet (fortsat) kan henvise borgere m.fl. til at rette henvendelse til et ”supplerende tilsyn”, og om Datatilsynet vil kunne omgøre afgørelser og beslutninger, der er truffet af et sådant tilsyn.

4. Anmeldelsespligt og tilladelseskrav

Det fremgår af lovforslagets § 26, stk. 1, at Datatilsynets tilladelse skal indhentes inden iværksættelse af en behandling, når behandlingen af oplysninger sker med henblik på 1) at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret, 2) behandlingen sker med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed eller 3) behandlingen udelukkende finder sted med henblik på at føre retsinformationssystemer.

Herudover fremgår det af lovforslagets § 7, stk. 4, at tilsynsmyndigheden giver tilladelse til privates behandling af følsomme oplysninger, som er nødvendig af hensyn til væsentlige samfundsinteresser, hvis behandlingen ikke foretages af eller for en offentlig myndighed.

Datatilsynet skal i den forbindelse henvise til databeskyttelsesforordningens præambelbetragtning nr. 89, hvoraf fremgår:

> ”Ved direktiv 95/46/EF blev der fastsat en generel forpligtelse til at anmelde behandlingen af personoplysninger til tilsynsmyndighederne. Denne forpligtelse medførte en administrativ og finansiel byrde, men den bidrog ikke i alle tilfælde til at forbedre beskyttelsen af personoplysninger. En sådan vilkårlig og generel anmeldelsespligt bør derfor afskaffes og erstattes med effektive procedurer og mekanismer, som i stedet fokuserer på de typer behandlingsak-

> tiviteter, der sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder i medfør af deres karakter, omfang, sammenhæng og formål. Sådanne typer behandlingsaktiviteter kan være aktiviteter, der navnlig indebærer brug af ny teknologi, eller aktiviteter som er af en ny slags, og hvor den dataansvarlige endnu ikke har foretaget en konsekvensanalyse vedrørende databeskyttelse, eller hvor de er blevet nødvendige på grund af den tid, der er gået siden den oprindelige behandling."

Under henvisning til det anførte i betragtningen – som Datatilsynet kan tilslutte sig – er tilsynet umiddelbart uforstående overfor, at der efter udkastet til lovforslag fortsat skal være en anmeldelsespligt på flere områder.

Det fremgår af bl.a. afsnit 2.6.3.1. i de almindelige bemærkninger til lovforslaget, at Justitsministeriet vurderer, at en sådan tilladelsesordning, kombineret med muligheden for at stille vilkår, jf. § 26, stk. 4, vil være egnet til at tilvejebringe et klart og utvetydigt grundlag, på hvilket virksomheden mv. kan foretage sin behandling.

Datatilsynet skal hertil bemærke, at tilsynet modtager mange henvendelser fra virksomheder mv., der har fået tilladelse til behandling af personoplysninger, om bl.a., hvorvidt konkrete behandlinger af både følsomme og ikke-følsomme personoplysninger er i overensstemmelse med persondataloven, og om hvordan konkrete situationer skal håndteres.

Det er på den baggrund tilsynets erfaring, at det ikke er muligt at forudse alle tilfælde, hvor behandling er aktuel. Det har således med tilladelsesordningen efter persondataloven i praksis ikke været muligt at tilvejebringe et klart og utvetydigt grundlag, på hvilket de enkelte virksomheder mv. har kunnet foretage deres behandlinger. Vilkårene i Datatilsynets tilladelser har derfor som udgangspunkt karakter af standardvilkår.

Datatilsynet skal på den baggrund foreslå, at der i stedet fastsættes en bemyndigelse for justitsministeren eller tilsynsmyndigheden til at fastsætte standardvilkår for behandling af personoplysninger på områder, hvor der måtte være behov herfor.

Datatilsynet skal i øvrigt pege på, at der i lovforslaget foreslås anmeldelses/tilladelsesordninger for privates behandling af oplysninger på fire områder (advarselsregistre, kreditoplysning, retsinformationssystemer samt behandling af artikel 9-oplysninger, der er nødvendig af hensyn til væsentlige samfundsinteresser).

De fire typer af tilladelsessager ses at blive reguleret på fire forskellige måder i lovforslaget:

Navnlig bemærkes, at behandling af artikel 9-oplysninger, der er nødvendig af hensyn til væsentlige samfundsinteresser, alene ses reguleret i lovforslagets § 7. Behandlingen er derimod ikke som de øvrige områder omfattet af § 26 i lovforslagets kapitel 9, der ellers bærer overskriften "Tilladelse til behandlinger, der foretages for en privat dataansvarlig".

Såfremt det til trods for ovennævnte bemærkninger fortsat vurderes, at der er behov for et tilladelseskrav på visse områder, skal Datatilsynet derfor opfordre til, at bestemmelserne herom ensrettes og samles, så der skabes større gennemsigtighed i forhold til, hvornår en tilladelse skal indhentes.

5. Afsluttende bemærkninger

Datatilsynet forudsætter at blive hørt i forbindelse med udarbejdelse af bekendtgørelser og andre generelle retsforskrifter i medfør af den vedtagne lov, jf. § 28 i udkastet til lovforslag.

Med venlig hilsen

Henrik Waaben	Cristina Angela Gulisano
Formand for Datarådet	Direktør

Det Sociale Netværk

Et initiativ under
Det Sociale Netværk
headspace

Justitsministeriet

databeskyttelseskontoret@jm.dk.

København, den 22. august 2017

Vedrørende høring over databeskyttelsesloven

Justitsministeriet har bedt om høringssvar til udkast til databeskyttelseslov. Her følger nogle overordnede betragtninger fra Det Sociale Netværk.

Vi har fuld forståelse for behovet for fælles regler, der giver enkelte personer tryghed og sikkerhed for at behandlingen af personfølsomme oplysninger hos offentlige myndigheder, virksomheder og organisationer foregår fuldt betryggende. Der har desværre været alt for mange tilfælde med sløset omgang med personfølesomme oplysninger. Det kan ingen være tjent med.

Omvendt er vi også meget usikre på hvad forslaget vil betyde for det frivillige foreningsDanmark.

Vi opfordrer derfor til, at det endelige regelsæt tager hensyn til de mange frivillige organisationer i Danmark, herunder de mange frivillige organisationer som ikke råder over store personaleressourcer eller besidder stor juridisk ekspertviden.

De mange frivillige drevne foreninger i Danmark har ikke brug for yderligere administrative byrder. Det vil være i modstrid med de tanker om en ny civilsamfundsstrategi som børne- og socialministeren arbejder på i øjeblikket. Samt ikke mindst i modstrid med regeringsgrundlagets formuleringer om at regeringen fremadrettet vil arbejde *"for, at der er de bedst mulige rammer for, at private organisationer og frivillige kan tage et medansvar"*

Der bør derfor tages et særligt hensyn til civilsamfundets mange organisationer i implementeringen af regelsættet.

Med venlig hilsen

Trine Hammershøy – direktør i Det Sociale Netværk / headspace

DFiR
DANMARKS FORSKNINGS- OG INNOVATIONSPOLITISKE RÅD

Til Justitsministeriet
Slotsholmsgade 10
1216 København K
att. Databeskyttelseskontoret

Danmarks Forsknings- og Innovationspolitiske Råd

22. august 2017

Børsgade 4
Post Postboks 2135
1015 København K
Tel. 3392 9700
Fax 3332 3501
Mail ufm@ufm.dk
Web www.ufm.dk

CVR-nr. 1680 5408

Ref.-nr. 17/003067-62

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

Danmarks Forsknings- og Innovationspolitiske Råd (DFiR) har fulgt arbejdet med EU's forordning om databeskyttelse og muligheden for fortsat at kunne anvende personfølsomme data til videnskabelige formål. Derfor er det med stor interesse, at rådet har læst forslag til databeskyttelsesloven. DFiR finder det særdeles positivt, at forordningen fastholder muligheden for at behandle personfølsomme data, hvis det er til videnskabelige formål. Der findes mange eksempler på banebrydende forskning, der har skabt ny og vigtig viden til gavn for samfundet, hvor forskningsresultaterne ikke havde haft samme kvalitet, hvis det ikke havde været muligt at anvende persondata i videnskabelige øjemed.

I lovforslaget er denne mulighed fastholdt på en hensigtsmæssig måde. Dog konstaterer DFiR, at det administrative set-up, der skal implementeres for at sikre forordningens krav til datatilsyn, kan risikere at blive uhensigtsmæssig bureaukratisk. DFiR understreger derfor, at man i den konkrete udmøntning af databeskyttelsesloven sikrer, at datasikringstiltag skal kunne fungere smidigt, hensigtsmæssigt og med forståelse for videnskabelige arbejdsgange.

Viden om hvilke udfordringer og muligheder, der er i forbindelse med at anvende personfølsomme data i videnskabeligt øjemed og andre sammenhænge, er afgørende at få inddraget i det arbejde, der jf. lovforslaget skal ske med datatilsyn. Nybrud i forskning indeholder ofte anvendelse af nye metoder og ny teknologi, herunder data. DFiR foreslår derfor, at et af medlemmerne af Datarådet jf. § 27 stk. 3 udpeges af uddannelse- og forskningsministeren med henblik på at inddrage indsigt i anvendelse af data til videnskabelige formål, men også for at have indsigt i, hvilke fremtidige tendenser, Datarådet må forventes at skulle forholde sig til.

Med venlig hilsen

Jens Oddershede
Formand for Danmarks Forsknings- og Innovationspolitiske Råd

Justitsministeriet
Slotsholmsgade 10
1216 København K

20. september 2017

J.nr.: 2017-4101-0044-40
Sagsbeh: Maiken Michelsen
Mail: MIMI@domstolsstyrelsen.dk

Domstolsstyrelsens høringssvar

Justitsministeriet har ved mail af 7. juli 2017 anmodet om eventuelle bemærkninger til udkast til forslag til databeskyttelseslov.

Det fremgår bl.a. af udkastet til lovforslaget, at EU den 14. april 2016 vedtog en såkaldt databeskyttelsespakke, som består af en generel forordning nr. 2016/679 om beskyttelse af personoplysninger, samt et direktiv om beskyttelse af personoplysninger. Forordningen skal anvendes fra den 25. maj 2018, og direktivet, som skal gælde for retshåndhævelsesområdet, er gennemført i dansk ret ved lov nr. 410 af 27. april 2017.

Udkastet til forslag til databeskyttelseslov fastsætter supplerende bestemmelser til databeskyttelsesforordningen om behandling af personoplysninger inden for det nationale råderum.

Domstolsstyrelsen har i høringssvar af 15. november 2015, 2. marts 2016 og 9. marts 2017 afgivet bemærkninger til forskellige dele af EU's databeskyttelsespakke.

Domstolsstyrelsen har i forhold til udkastet til databeskyttelseslov følgende bemærkninger:

Det følger af lovforslagets § 22, stk. 1, nr. 6, at undtagelse fra bestemmelserne i databeskyttelsesforordningens artikel 12-15 om oplysningspligt og indsigtsret kan gøres, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige interesser, herunder bl.a. beskyttelse af retsvæsenets uafhængighed og retssager. I bemærkningerne til bestemmelsen er det bl.a. anført, at indskrænkningen i oplysningspligten kun kan ske på grundlag af en konkret afvejning af de modstående interesser, der er nævnt i bestemmelsen, som fx beskyttelse af retsvæsenets uafhængighed og retssager, og at det med anvendelsen af udtrykket "afgørende" er tilkendegivet, at undtagelsen fra oplysningspligten kun kan gøres, hvor der er nærliggende fare for, at offentlige interesser vil lide skade af væsentlig betydning. Således som Domstolsstyrelsen forstår bemærkningerne, kan undtagelser fra oplysningspligten efter lovforslaget således alene ske på baggrund af en konkret bedømmelse af de enkelte situationer.

Domstolsstyrelsen vil foreslå, at der i loven fastsættes generelle undtagelser fra oplysningspligten og indsigtsretten for så vidt angår oplysninger, der behandles af domstolene i forbindelse med deres judicielle virksomhed. Der henvises i den forbindelse til indholdet af forordningens præambelbetragtning nr. 20, hvoraf det bl.a. fremgår, at selv om forordningen bl.a. finder anvendelse på domstoles og andre judicielle myndigheders aktiviteter, kan EU-retten eller medlemsstaternes nationale ret præcisere, hvilke behandlingsaktiviteter og -procedurer, der finder anvendelse i forbindelse med domstoles og andre judicielle myndigheders behandling af personoplysninger.

Det bemærkes, at Domstolsstyrelsen ikke hermed har taget stilling til anvendelsesområdet for databeskyttelsesforordningens artikel 14.

Domstolsstyrelsen bemærker endelig, at lovforslaget ikke indeholder overvejelser om de ressourcemæssige konsekvenser, herunder eventuelle udgifter forbundet med krav om logning m.v., som følger af lovforslaget. Domstolsstyrelsen tager derfor forbehold for udgifter i forbindelse hermed.

Med venlig hilsen

Charlotte Münter

Danmarks Tekniske Universitet

Justitsministeriet
Lovafdelingen

25. august 2017

DTU's bemærkninger til udkast til forslag til databeskyttelsesloven

Justitsministeriet har den. 7. juli 2017 sendt ovennævnte lovforslag i høring.

DTU anser det for positivt, at forslaget overordnet set synes at sigte efter en videreførelse af den aktuelle tilstand.

De aktuelle regler er godt integreret i DTU's aktiviteter, og en videreførelse vil derfor indebære, at DTU i vidt omfang kan implementere forordningen ved at bygge videre på de etablerede arbejdsgange.

DTU har særligt forholdt sig til forslaget om brug af data til forskning og til spørgsmålet om bøde til offentlige myndigheder.

Forskningsreglen i § 10 og udveksling af data
DTU har noteret sig, at forslaget efter § 10 indebærer, at der fortsat kræves tilladelse til en videregivelse af data samt, at Datatilsynet fortsat får mulighed for at give en generel tilladelse til videregivelse.

En væsentlig del af DTUs forskningsprojekter er bygget op som samarbejder med andre institutioner eller virksomheder. For at disse samarbejder skal nå deres fulde potentiale, skal der ske en udveksling af data, men de aktuelle regler står i vejen for at potentialet kan udnyttes ordentligt.

Behovet for at kunne udveksle data inden for solide og sikre juridiske rammer vokser. Der kommer flere og flere forskningsprojekter, som bygger på "smart"-teknologier som via f.eks. biler, boliger og infrastruktur giver adgang til at indsamle betragtelige mængder af data. Samtidig får forskningsprojekterne en størrelse, så den enkelte forskningsinstitution ikke kan løfte opgaven alene.

Danmark har en førerposition inden for forskning i data fra "smart"-teknologier. Den førerposition har vi bl.a., fordi vi har adgang til mange og gode data. Hvis vi skal opretholde den førerposition, er det nødvendigt, at der også kommer ordentlige muligheder for at udveksle data med andre institutioner inden for de enkelte forskningsprojekter, med juridiske rammer der giver reel tryghed for de registrerede personer og bidrager til sikring af deres rettigheder.

Danmarks Tekniske Universitet
Ledelse og Administration
Anker Engelunds Vej 1
Bygning 101
2800 Kgs. Lyngby
Tlf. 45 25 25 25
direktor@adm.dtu.dk
www.dtu.dk

Efter det aktuelle system kan vi *de facto* vælge mellem at udveksle data under en databehandleraftale eller efter en aftale om videregivelse.

Begge modeller kræver at meget formalistisk set-up. Konsekvensen er, at universiteterne bruger unødvendigt mange ressourcer på at skabe og vedligeholde de formelle juridiske rammer for udveksling af data, uden at disse rammer bidrager til øget sikkerhed for de registreredes rettigheder.

DTU foreslår derfor, at der i loven skabes hjemmel til en mere enkel og mindre formalistisk adgang til at udveksle data mellem offentlige forskningsinstitutioner til brug for forskning, jf. nærmere neden for.

Databehandler
Rollen som databehandler harmonerer dårligt med de øvrige regler, som DTU arbejder under i forskningsprojekter: efter de almindelige bevillingsmæssige regler, skal DTU have en forskningsmæssig interesse i de samfinansierede forskningsaktiviteter vi deltager i, og efter reglerne for databehandling, må vi ikke have en egeninteresse i behandlingen af data, hvis vi er databehandler. Der er altså et grundlæggende modsætningsforhold.

Hvis DTU behandler data som databehandler, kan den dataansvarlige kræve, at DTU sletter de relevante data. Konsekvensen er, at DTU er nødt til at stoppe forskningsprojektet i utide, hvilket typisk i praksis vil betyde, at den udførte forskning bliver værdiløs. Kravet om sletning indebærer også, at det kan være umuligt at leve op til reglerne for god forskningsskik, fordi der i disse regler er et krav om, at man skal kunne dokumentere sine data.

Databehandlerkonstruktionen forudsætter desuden et formalistisk set-up med aftaler og mange "lag" af sikkerhedspolitikker og kontrolprocesser, som i denne sammenhæng reelt ikke forbedrer sikkerhed for de registrerede – særligt ikke når både databehandler og dataansvarlig er danske offentlige institutioner.

I praksis ses databehandlerkonstruktionen især anvendt i en uhensigtsmæssig sammenhæng, når der er tale om sundhedsdata, hvor sundhedslovens § 46 forhindrer videregivelse, med mindre Styrelsen for Patientsikkerhed har godkendt videregivelsen. Styrelsens sagsbehandlingstid vil ofte indebære, at videregivelse af sundhedsdata ikke kan gennemføres inden for et projekts løbetid.

DTU foreslår på den baggrund, at man i forbindelse med implementeringen af forordningen også tager stilling til bestemmelsen om videregivelse af sundhedsdata i sundhedslovens § 46 og justerer denne bestemmelse, så der bliver en mere enkel adgang til videregivelse af sundhedsdata fra regionerne til universiteterne og universiteterne imellem.

Videregivelse
Videregivelse af data harmonerer bedre med de bevillingsmæssige regler end modellen med overdragelse under en databehandleraftale.

Men også videregivelse kræver et meget omfattende formalistisk forarbejde, som ikke forbedrer sikkerheden for de registrerede, når der er tale om videregivelse mellem forskningsinstitutioner.

Aktuelt er der krav om, at universiteterne dels sikrer en erklæring fra modtageren af data om overholdelse af en række vilkår, dels dokumenterer tilladelsen til videregivelse. Hvis der er tale om videregivelse til udlandet (herunder EU), skal der indhentes konkret tilladelse fra Datatilsynet, hvilket pga. sagsbehandlingstiden i praksis kan forhindrer videregivelse.

DTU foreslår, at lovforslaget om databeskyttelsesloven tilføjes en generel adgang til videregivelse af data til forskningsmæssige formål mellem danske forskningsinstitutioner frem for som foreslået i udkastet at opretholde det gældende krav om tilladelse fra Datatilsynet. Adgangen til videregivelse kunne f.eks. konkretiseres i en bekendtgørelse.

DTU foreslår endvidere, at adgangen til videregivelse ikke gøres betinget af udveksling af diverse erklæringer og dokumentation for opfyldelse af krav, som parterne efter loven under alle omstændigheder er forpligtede til at overholde.

DTU foreslår endelig, at ministeriet undersøger mulighederne for at inddrage videregivelse til andre universiteter i EU i den generelle adgang til at videregive data.

Fælles dataansvar

Aktuelt giver loven også en mulighed for at udveksle data ved at etablere et fælles dataansvar, men praksis er restriktiv.

Et fælles dataansvar ville harmonere bedre med de mange forskningsprojekter, hvor flere parter i fællesskab bearbejder og forbedrer data, og hvor der er en fælles adgang til at disponere over data.

Fælles dataansvar synes at rumme muligheden for, at parterne etablerer en struktur for håndteringen af data i det konkrete forskningsprojekt, som dels sikrer en klar fordeling af ansvar og opgaver, dels sikrer at dataenes forskningsmæssige potentiale kan udnyttes optimalt, dels skaber en reel sikkerhed for de registreredes rettigheder.

Men efter den aktuelle praksis er fælles dataansvar ikke en reel mulighed pga. kravet om en konkret tilladelse og Datatilsynets restriktive praksis. Denne praksis har i sagens natur også betydet, at ingen af universiteterne har investeret ressourcerne i at afdække muligheden for at skabe et solidt grundlag for fælles dataansvar.

Som det fremgår af betænkningen, indebærer forordningens art 26 reelt ikke en ændring af den aktuelle danske retstilstand og betænkningen og lovforslaget lægger ligeledes ikke op til en ændring af praksis for Datatilsynets håndtering af spørgsmål om fælles dataansvar, da der er forbundet en række udfordringer med det fælles dataansvar.

DTU foreslår, at ministeriet undersøger muligheden for at tillade forskningsprojekter med fælles dataansvar nærmere, og at der om muligt udarbejdes konkrete retningslinjer for håndteringen af fælles dataansvar.

Bødeansvar

I forhold til spørgsmålet omkring bødeansvar for offentlige myndigheder, foreslår DTU, at offentlige forskningsinstitutioner holdes fri for bødeansvar.

Det er vores helt grundlæggende opfattelse, at de ressourcer som DTU disponerer over, skal bruges til at skabe og formidle nye indsigter – og ikke til at betale eventuelle bøder.

Offentlige myndigheders bevillinger er tildelt til specifikke formål og bødesanktioner vil påvirke myndighedens mulighed for at gennemføre opgaver, de er pålagt ved lov. Det gælder uanset om opgaven er indskrivning på studier, tildeling af grader, personaleadministrative opgaver, økonomistyring o.l.

DTU har forståelse for, at der kan være et ønske om at opnå en præventiv virkning ved at skabe grundlag for bøder, men det er min vurdering, at det greb vil være forfejlet i forhold til universiteterne.

Den ovenfor beskrevne disharmoni mellem de aktuelle muligheder for udveksling af data og den praktiske virkelighed i forskningsprojekter, indebærer, at der er en vis risiko for, at myndighederne vil vurdere, at reglerne ikke bliver efterlevet.

Samtidig har DTU en meget væsentlig egeninteresse i at sikre, at de data DTU arbejder med i forbindelse med forskningsprojekter, behandles på en måde, så risikoen for de registrerede personer er mindst mulig. Der er også generelt en meget høj grad af opmærksomhed i forskningsmiljøerne på, at adgangen til at arbejde med persondata bygger på et særligt lovgivningsmæssigt privilegium, som fordrer en høj grad af ansvarlighed. Den reelle datasikkerhed er derfor høj.

DTU mener derfor ikke, at et bødeansvar inden for forskningsområdet vil bidrage til øget datasikkerhed og til at mindske risikoen for de registrerede personer.

Vi står naturligvis til rådighed, såfremt ministeriet har et ønske om at få uddybet nogle af de anførte bemærkninger.

Med venlig hilsen

Claus Nielsen
Universitetsdirektør

Fra: CAS - Digitalisering (Fællespostkasse) [Digitalisering@egekom.dk]
Sendt: 23. august 2017 11:56
Til: Justitsministeriet
Cc: Anders Lungholt; Jette Bondo; CAS - Digitalisering (Fællespostkasse)
Emne: SV: Høring over udkast til forslag til databeskyttelsesloven - (2016-7910-0021)

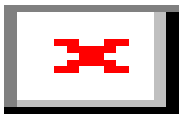
Til Justitsministeriet

Egedal Kommune har ingen bemærkninger til høringen over lovforslag til databeskyttelsesloven (2016-7910-0021)

Med venlig hilsen

Jens Sønderbye Kjærulff
Informationssikkerhedskoordinator

Digitalisering og Effektivisering
Center for Administrativ Service
Mobilnummer: 7259 6240
E-mail: Jens.Kjaerulff@egekom.dk
www.egedalkommune.dk



Fra: Justitsministeriet [mailto:jm@jm.dk]
Sendt: 28. juli 2017 10:54
Til: 'post@aabenraa.dk'; Aalborg Kommune – Folkeregisteret; 'law@law.aau.dk'; 'post@aarhus.dk'; 'post@aarhusretshjaelp.dk'; 'ekspedition.law@au.dk'; 'samfund@advokatsamfundet.dk'; 'ac@ac.dk'; Albertslund Kommune; Allerød Kommune; 'amnesty@amnesty.dk'; 'abf@abf-rep.dk'; 'ae@ae.dk'; 'mail@arkitektforeningen.dk'; 'assens@assens.dk'; 'pote@atp.dk'; 'balkom@balk.dk'; Beskæftigelsesmin.; 'kommunen@billund.dk'; 'bl@bl.dk'; 'post@brk.dk'; 'brondby@brondby.dk'; 'raadhus@99454545.dk'; Socialmin.; 'cbs@cbs.dk'; 'bl@bl.dk'; 'dif@dif.dk'; 'djoef@djoef.dk'; 'dl@dklf.dk'; 'journalen@dr.dk'; 'dtu@dtu.dk'; 'da@da.dk'; 'info@danskbyggeri.dk'; 'de@de.dk'; 'hoeringssager@danskerhverv.dk'; 'dfs@dfs.dk'; 'di@di.dk'; 'adm@nodeco.dk'; 'dit@dit.dk'; 'dj@journalistforbundet.dk'; 'info@danske-aeldreraad.dk'; 'mail@danskeadvokater.dk'; 'cbh@danskeforlag.dk'; 'dh@handicap.dk'; 'forening@danskeadvokater.dk'; 'mail@danskemedier.dk'; 'regioner@regioner.dk'; 'info@danske-seniorer.dk'; 'kontakt@danskeudlejere.dk'; 'dt@datatilsynet.dk'; 'dommerforeningen@gmail.com'; 'dch@dch.dk'; 'office@voldgiftsinstituttet.dk'; 'dkr@dkr.dk'; $Direktoratet for Kriminalforsorgen; 'hoeringer@dommerfm.dk'; 'pibr@domstol.dk'; 'post@domstolsstyrelsen.dk'; Dragør Kommune; Egedal Kommune; 'info@ejendomsforeningen.dk'; 'efkm@efkm.dk'; 'mail@envina.dk'; 'pm@adv-martinelli.dk'; 'evm@evm.dk'; 'raadhuset@esbjergkommune.dk';

'experian@experian.dk'; Faaborg-Midtfyn Kommune; 'post@fabnet.dk'; 'raadhuset@fanoe.dk'; 'favrskov@favrskov.dk'; 'kommunen@faxekommune.dk'; 'post@finansogleasing.dk'; 'fm@fm.dk'; 'mail@finansraadet.dk'; 'foa@foa.dk'; 'forbrugerombudsmanden@kfst.dk'; 'fbr@fbr.dk'; 'lsc@ankl.dk'; Statsadvokaten i København; 'lcanor@statsforvaltningen.dk'; 'pup@plesner.com'; 'fp@forsikringogpension.dk'; 'fk@fmf.dk'; 'fmn@fmn.dk'; Fredensborg Kommune; 'kommunen@fredericia.dk'; 'raadhuset@frederiksberg.dk'; 'post@frederikshavn.dk'; 'epost@frederikssund.dk'; 'fsr@fsr.dk'; 'ftf@ftf.dk'; 'furesoe@furesoe.dk'; 'sekretatiatet@grundejeren.dk'; 'info@tinganes.fo'; Gentofte Kommune; 'kommunen@gladsaxe.dk'; 'glostrup.kommune@glostrup.dk'; 'raadhus@greve.dk'; 'gribskov@gribskov.dk'; 'info@nanoq.gl'; Guldborgsund Kommune; 'post@haderslev.dk'; Halsnæs Kommune; 'au@au.dk'; 'nyhedensted@hedensted.dk'; 'mail@helsingor.dk'; 'herlev@herlev.dk'; 'kommunen@herning.dk'; 'hillerod@hillerod.dk'; 'hjoerring@hjoerring.dk'; 'hk@hk.dk'; 'hovedstaden@hk.dk'; 'sammail@holbkom.dk'; 'horsens.kommune@horsens.dk'; 'hvidovre@hvidovre.dk'; 'post@hoejesteret.dk'; Høje-Taastrup Kommune; 'kommunen@horsholm.dk'; 'hvr@hvr.dk'; 'post@ikast-brande.dk'; 'isobro@isobro.dk'; 'ida@ida.dk'; 'info@humanrights.dk'; Ishøj Kommune; 'itb@itb.dk'; 'raadhus@jammerbugt.dk'; 'info@justitia-int.org'; 'kalundborg@kalundborg.dk'; 'kommune@kerteminde.dk'; 'km@km.dk'; 'kl@kl.dk'; 'raadhus@kolding.dk'; 'info@kreakom.dk'; 'info@cancer.dk'; 'kum@kum.dk'; 'kobenhavn@domstol.dk'; 'borgerservice@kk.dk'; 'jurfak@jur.ku.dk'; 'raadhus@koege.dk'; 'pt@strafferetsadvokaten.dk'; 'krim@krim.dk'; 'vnn.stat@hktillidsvalgt.dk'; 'lo@lo.dk'; 'post@langelandkommune.dk'; 'llodk@llodk.dk'; Lemvig Kommune; 'kmr@ac.dk'; 'lolland@lolland.dk'; Lyngby-Taarbæk Kommune - borgerservice; 'dadl@dadl.dk'; 'info@lif.dk'; 'kommunen@laesoe.dk'; 'raadhus@mariagerfjord.dk'; 'middelfart@middelfart.dk'; 'mim@mim.dk'; 'fmn@fmn.dk'; 'kommunen@morsoe.dk'; 'nmkn@nmkn.dk'; 'norddjurs@norddjurs.dk'; Nordfyns Kommune; 'kommune@nyborg.dk'; 'borger@naestved.dk'; 'odder.kommune@odder.dk'; Odense Kommune; Odsherred Kommune; 'sekretariat@parcelhus.dk'; 'lfr001@politi.dk'; 'mail@politiforbundet.dk'; 'skrivpost@postnord.com'; 'post@procesbevillingsnaevnet.dk'; 'prosa@prosa.dk'; 'randerskommune@randers.dk'; 'mail@realkreditforeningen.dk'; 'rkr@rkr.dk'; 'raadhus@rebild.dk'; 'info@shipowners.dk'; 'formand@retspolitik.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'; 'holbaek@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'; 'riomgr@gl.stm.dk'; 'ro@fo.stm.dk'; 'politi@politi.dk'; 'post@rksk.dk'; 'ringsted@ringsted.dk'; 'kommunen@roskilde.dk'; 'rudersdal@rudersdal.dk'; Rødovre Kommune; 'info@digitalsikkerhed.dk'; 'rem@siri.dk'; 'slrtv@slrtv.dk'; Samsø Kommune; 'ksm@sikkerhedsbranchen.dk'; 'kommunen@silkeborg.dk'; Skanderborg Kommune; 'skm@skm.dk'; Skive Kommune; 'slagelse@slagelse.dk'; 'kommune@solrod.dk'; Sorø Kommune; 'stm@stm.dk'; 'stevns@stevns.dk'; 'struer@struer.dk'; 'sum@sum.dk'; 'svendborg@svendborg.dk'; 'sdu@sdu.dk'; Syddjurs Kommune; 'post@shret.dk'; 'post@sonderborg.dk'; 'thistedkommune@thisted.dk'; 'ssha@domstol.dk'; 'trm@trm.dk'; 'jura@tv2.dk'; 'toender@toender.dk'; Tårnby Kommune; 'hfa@ac.dk'; 'ufm@ufm.dk'; 'um@um.dk'; 'uim@uim.dk'; 'uvm@uvm.dk'; 'raadhus@vallensbaek.dk'; 'vardekommune@varde.dk'; 'post@vejenkom.dk'; Vejle Kommune; 'post@vesthimmerland.dk'; 'post@vestrelandsret.dk'; 'viborg@viborg.dk'; 'post@vordingborg.dk'; 'aeldresagen@aeldresagen.dk'; 'aef@aeldreforum.dk'; 'post@aeroekommune.dk'; 'oim@oim.dk'; 'post@oestrelandsret.dk'; '3f@3f.dk'; dfs@dfs.dk; plj@fmf.dk; arsmad@statsforvaltningen.dk; hip001@politi.dk; faglig@prosa.dk
Emne: Høring over udkast til forslag til databeskyttelsesloven - (2016-7910-0021)

Justitsministeriet skal anmode om, at eventuelle bemærkninger til udkast til forslag til databeskyttelsesloven sendes til databeskyttelse@jm.dk.

Med venlig hilsen

Nanna Due Binø
Fuldmægtig

Databeskyttelseskontoret
Slotsholmsgade 10
1216 København K
Tlf. direkte: 72268828
Tlf.: 7226 8400
www.justitsministeriet.dk
jm@jm.dk

Alene fremsendt pr. e-mail: databeskyttelse@jm.dk
Justitsministeriet
Lovafdelingen
Slotsholmsgade 10
1216 København K

Att.: Databeskyttelseskontoret

22. august 2017
Juridisk konsulent, advokat
Mette Haagensen
Telefon +45 33 12 03 30
meh@ejendomsforeningen.dk

Bemærkninger til udkast til forslag til databeskyttelsesloven

Justitsministeriet har i brev af 7. juli 2017 anmodet om Ejendomsforeningen Danmarks bemærkninger til udkast til forslag til databeskyttelsesloven.

Overordnet er det Ejendomsforeningen Danmarks holdning, at man bør være særdeles tilbageholdende med at supplere et EU-regelsæt på forordningsniveau med yderligere national lovgivning. Regulering på forordningsniveau skal netop sikre, at implementering og håndhævelse sker ensartet i alle EU´s medlemslande. Dette formål bliver tilsidesat, hvis Danmark ved siden af forordningen ønsker at opretholde sin egen supplerende regulering. Denne ekstra regulering, som synes båret af et ønske om at bibeholde retstilstanden efter den gamle registerlovgivning, kan medføre en konkurrenceforvridning på tværs af landegrænser, hvor danske virksomheder mister konkurrenceevne, som følge af skrappere regler.

Ejendomsforeningen Danmark skal i den forbindelse bemærke, at det er stødende over for de private virksomheder, der ser ind i en regulering med væsentlig forhøjelse af bødestørrelsen, at man ikke har ønsket at tage stilling til offentlige myndigheders bødeniveau. Ejendomsforeningen Danmark kan frygte, at den manglende adressering af bødeniveauet skaber det forkerte incitament hos de offentlige myndigheder, således at der ikke på ledelsesniveau kommer tilstrækkelig fokus på, at man også som offentlig myndighed må stå på mål for at leve op til databeskyttelseslovgivningen. En afledt effekt heraf kan være en øget risiko for erstatningsansvar hos de offentlige myndigheder, idet erstatningsansvaret både gælder private virksomheder og offentlige myndigheder.

Ejendomsforeningen Danmark har forståelse for, at man ønsker en let adgang til datadeling i den offentlige forvaltning for at sikre en effektiv sagsbehandling, men Ejendomsforeningen Danmark kan frygte at indførelse af undtagelsen i § 5, stk. 3 om muligheden for at viderebehandle personoplysninger til andre formål en oprindeligt oplyst kan medføre uheldige følger. I Ejendomsforeningen Danmark har vi allerede set eksempler på, at de kommunale folkeregistre forsøger at strække hjemmelsgrundlaget i lov om Det centrale

Personregister (CPR-loven) § 10, stk. 2 langt udover, hvad der er rimeligt og måske endda lovligt. Vores medlemmer har således flere gange oplevet, at folkeregistrene har bedt vores medlemmer (udlejere og administratorer) om at verificere følsomme oplysninger om lejernes personlige forhold, som udlejer under normale forhold ikke ville have en saglig interesse i at registrere. Det er derfor bekymrende for den registrerede borger, hvis en offentlig myndighed kan få hjemmel til at benytte persondata til andet end det, der udtrykkeligt har været formålet med indsamlingen oprindeligt - og dette endda uden at den registrerede bliver oplyst om, at man nu benytter persondataene til et andet formål.

Man har i § 2, stk. 5 indført, at persondatalovgivningen skal finde anvendelse på afdøde personer i 10 år efter vedkommendes død. I Ejendomsforeningen Danmark savner vi, at man ved indførelsen af disse regler tillige har taget stilling til, hvem der i disse 10 år kan udøve den registreredes rettigheder. Vil et dødsbo fx kunne indtræde i disse rettigheder og bede om indsigt? Hvis ja, hvad sker der når dødsboet er afsluttet? Når den registrerede er afgået ved døden, og den dataansvarlige i henhold til persondatalovgivningen skal overholde sin oplysningspligt, hvem skal den dataansvarlige give disse oplysninger til?

Dette er blot nogle få konkrete overvejelser i forhold til den særregulering man ønsker at indføre i Danmark i forhold til andre EU-lande på trods af, at vi har forpligtet os til gennemføre og anvende forordningen på en ensartet måde i hele EU, jf. forordningen artikel 61, stk. 1, 1 pkt.

Venlig hilsen

Morten Østrup Møller
Juridisk direktør

ERHVERVSSTYRELSEN

21. august 2017
TEAM JURA
/ChrGar-erst

Sagsnr. 2017-8077

Erhvervsstyrelsens høringssvar vedrørende databeskyttelsesloven

Erhvervsstyrelsen har modtaget høring vedr. databeskyttelsesloven.

Nedenfor ses høringssvar fra Team Effektiv Regulering (TER).

Team Effektiv Regulering (TER)
TER vurderer, at lovforslaget ikke i sig selv medfører administrative konsekvenser for erhvervslivet, da der ikke indføres yderligere krav om dokumentation end dem, der følger af databeskyttelsesforordningen. Kravene om fx udvidelse af oplysningspligten, udarbejdelse af konsekvensanalyser, underretning af tilsynsmyndighederne mv., er krav, der tilsammen medfører væsentlige administrative byrder for erhvervslivet, men som følger direkte af databeskyttelsesforordningen. Konsekvenserne skal derfor ikke opgøres her, da de ikke hidrører fra nærværende lovforslag.

TER vurderer på den baggrund, at lovforslaget ikke medfører administrative konsekvenser for erhvervslivet.

Kontaktperson vedr. ovenstående bemærkninger:

Thomas Tolstrup Jensen
Fuldmægtig
Tlf. Direkte: 3529 1885
E-post: ThoTol@erst.dk

Med venlig hilsen

Christina Gardshodn
Stud.jur., Team Jura
Erhvervsstyrelsen
Tlf.: +45 3529 1355
E-mail: chrgar@erst.dk

ERHVERVSSTYRELSEN
Dahlerups Pakhus
Langelinie Allé 17
2100 København Ø

Tlf 35 29 10 00
Fax 35 46 60 01
CVR-nr. 10 15 08 17
erst@erst.dk
www.erst.dk

Experian A/S
CVR nr. 63 67 09 28
Lyngbyvej 2
DK-2100 København Ø
T: +45 70 10 01 07
E: experian@experian.dk
www.experian.dk

Justitsministeriet
Databeskyttelseskontoret
Slotsholmsgade 10
1216 Købehavn K

Sendt pr. e-mail: databeskyttelseskontoret@jm.dk

København, den 22. august 2017

Høringssvar – udkast til forslag til databeskyttelseslov

Justitsministeriet har den 7. juli 2017 sendt udkast til forslag om databeskyttelsesloven i høring med høringsfrist den 22. august 2017.

Experian A/S skal hermed fremkomme med følgende bemærkninger og kommentarer:

Ved en gennemgang af det fremlagte udkast har Experian A/S noteret sig, at de danske særregler og praksis for kreditoplysningsbureauvirksomhed stort set videreføres uændret i den nye databeskyttelseslov, herunder blandt andet kravet om indhentelse af forudgående tilladelse fra Datatilsynet, og Datatilsynets adgang til at fastsætte særskilte vilkår i forbindelse med meddelelse af sådan tilladelse.

Experian A/S ønsker, at Datatilsynet foretager høring af branchen og de berørte parter i forbindelse med udarbejdelsen af forslag til nye standardvilkår for kreditoplysningsbureauer som hjemlet i den nye databeskyttelseslov.

- - o0o - -

Experian A/S står naturligvis til rådighed, hvis dette høringssvar giver anledning til spørgsmål eller bemærkninger.

Med venlig hilsen
Experian A/S

Mikael Boldt Christensen
Advokat

Justitsministeriet
Slotsholmsgade 10
1216 København K.

Sendt til: databeskyttelse@jm.dk

FINANS DANMARK

Høringssvar vedrørende udkast til forslag til databeskyttelsesloven

Høringssvar

22. august 2017
Dok. nr. 572630-v1

Resumé

Databeskyttelsesloven har til formål at supplere og gennemføre persondataforordningen, og dermed ophæves den nugældende persondatalov.

Justitsministeriet har anført, at der i vidt omfang er tale om en videreførelse af de gældende regler. Ikke desto mindre giver det ændrede regelgrundlag anledning til en række spørgsmål, herunder om det fremadrettede tilsyn og rækkevidden af de nye regler.

Det skal også fremadrettet være Datatilsynet, der fører det generelle tilsyn med overholdelsen af persondatareglerne, mens særmyndigheder som eksempelvis Finanstilsynet udgør et supplerende tilsyn. Det er afgørende, at der sikres en klar ansvars- og kompetencefordeling på områder, hvor der kan være flere kompetente myndigheder. Det er ligeledes afgørende for et effektivt tilsyn, at der afsættes tilstrækkelige ressourcer til Datatilsynet, da det bedste tilsyn opnås, når der er ressourcer til at indgå i aktiv dialog med interessenterne frem for blot at reagere på konkrete situationer.

I forhold til behandling af data – og særligt behandling af følsomme personoplysninger – savner Finans Danmark større klarhed over konsekvenserne af den nye regulering. Det er ikke usædvanligt, at finansielle virksomheder behandler følsomme oplysninger som en del af afgørelsesgrundlaget i konkret sagsbehandling. Det er afgørende, at der også fremadrettet er den fornødne hjemmel til disse behandlinger, som udgør en integreret del af forretningen, og som forventes af kunderne.

Derudover giver lovforslaget anledning til en række konkrete bemærkninger i forhold til øvrige behandlingsregler, lovens anvendelsesområde samt sanktionsspørgsmålet.

Justitsministeriet har sendt udkast til forslag til databeskyttelsesloven i høring 7. juli 2017. Loven har til formål at supplere reglerne i databeskyttelsesforordningen og skal sammen med forordningen afløse lov om behandling af personoplysninger ved ikrafttræden den 25. maj 2018.

Lovforslaget giver Finans Danmark anledning til en række bemærkninger, som fremgår nedenfor. Der er tale om kompleks regulering, der som beskrevet er nært forbundet med databeskyttelsesforordningen. Finans Danmark fokuserer i høringssvaret på lovforslaget, hvorimod spørgsmål og

kommentarer, der vedrører databeskyttelsesforordningen, vil blive adresseret i anden sammenhæng.

Lovens geografiske område

Det følger af bemærkningerne til forslagets § 4, at bestemmelsen lægger sig helt op ad det geografiske anvendelsesområde for forordningen, således at det geografiske område for forordningen og loven er sammenfaldende.

Loven gælder for behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i Danmark. Derudover gælder loven for visse behandlingsaktiviteter i forhold til registrerede, der befinder sig i Danmark, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i EU.

Heroverfor står databeskyttelsesforordningen, som efter artikel 3, stk. 1, gælder for behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i EU.

Finans Danmark forstår dette således, at loven efter det foreslåede ikke finder anvendelse i det tilfælde, hvor en dataansvarlig eller en databehandler er etableret i et andet EU-land end Danmark – uanset at den registrerede befinder sig i Danmark. I de situationer gælder alene databeskyttelsesforordningen og eventuel national regulering i det pågældende EU-land.

Det afgørende i forhold til vurderingen af, hvilken regulering der finder anvendelse, bliver, hvorvidt den dataansvarlige er "etableret" i Danmark. Det står ikke Finans Danmark fuldstændig klart, hvornår en dataansvarlig kan siges at være etableret i Danmark i henhold til databeskyttelsesretten, og Finans Danmark skal derfor opfordre til, at dette gøres mere klart i lovgivningen.

Spørgsmålet om etablering får eksempelvis betydning i relation til den danske særregel om markedsføring i lovforslagets § 13. Finans Danmark er bekymret for, at lovforslagets § 13 sammenholdt med § 4 betyder, at virksomheder, der er etableret i EU, men ikke i Danmark, ikke er underlagt samme restriktive regler for behandling af oplysninger i forbindelse med markedsføring som virksomheder, der er etableret i Danmark. Finans Danmark skal i den forbindelse erindre om principperne for implementering af erhvervsrettet EU-regulering, hvoraf blandt andet følger, at danske virksomheder ikke bør stilles dårligere i den internationale konkurrence, hvorfor implementeringen ikke bør være mere byrdefuld end den forventede implementering i sammenlignelige EU-lande.

Det er helt afgørende, at danske særregler på databeskyttelsesområdet ikke kommer til at virke konkurrenceforvridende.

Behandling af oplysninger

Følsomme oplysninger

Hjemlen til behandling af følsomme oplysninger følger dels direkte af databeskyttelsesforordningen og dels af særlige bestemmelser i lovforslaget. Det fremgår af bemærkningerne til lovforsla-

gets § 7, at der efter Justitsministeriets opfattelse i meget vidt omfang efter databeskyttelsesforordningens artikel 9, stk. 2, litra a, c, d, e og f, vil kunne behandles følsomme oplysninger i samme omfang, som det er tilfældet i dag efter persondatalovens § 7, stk. 2 og 4.

Overgangen fra national regulering i persondataloven til EU-regulering i databeskyttelsesforordningen giver dog anledning til spørgsmål om rækkevidden af den fremtidige behandlingshjemmel set i forhold til den nugældende. Dette gælder eksempelvis i forhold til artikel 9, stk. 2, litra f, om retskrav, hvor den beskrivelse, der fremgår af betænkningen, altovervejende er fokuseret på offentlige myndigheders muligheder for behandling af data. Der mangler tilsvarende fortolkningsbidrag i forhold til private dataansvarlige, og Finans Danmark skal opfordre til, at der skabes øget klarhed på dette område. Selvom finansielle virksomheder ikke leverer en ydelse, der altid er knyttet sammen med følsomme oplysninger, udgør disse ofte en integreret del af afgørelsesgrundlaget.

Særligt på pensionsområdet behandler pengeinstitutter – som andre finansielle virksomheder – helbredsoplysninger regelmæssigt. For så vidt angår persondatalovens § 7, stk. 2, nr. 4, der svarer til forordningens artikel 9, stk. 2, litra f, fremgår det af betænkningens side 202, at retskravshjemlen eksempelvis vil gælde for forsikringsselskabers behandling af helbredsoplysninger med henblik på at vurdere, om den registrerede har krav på erstatning.

Finans Danmark forudsætter, at behandlingshjemlen i forordningens artikel 9, stk. 2, litra f, tilsvarende finder anvendelse i forhold til finansielle virksomheders behandling af følsomme oplysninger i forbindelse med pensionsadministration og pensionsudbetaling, eksempelvis i den situation, hvor en pensionskunde af helbredsmæssige årsager anmoder om at få udbetalt sin pensionsordning før tid.

I modsat fald er der efter Finans Danmarks opfattelse behov for at skabe hjemmel til en enkel og smidig behandling af helbredsoplysninger i forbindelse med pensioner, uden at der behøver at foreligge et udtrykkeligt samtykke. Kundernes oplysninger vil i den forbindelse være beskytter af reglen i lov om finansiel virksomhed § 119, som sikrer, at videregivelse ikke kan ske uden samtykke, ligesom det bør sikres, at anvendelse af oplysningerne til andre formål er forbudt.

Endelig bemærkes, at Finans Danmark er enig i det anførte nederst på side 266 i lovforslaget om, at det kan være vanskeligt på forhånd fuldstændigt at forudse behovet for at kunne behandle personoplysninger omfattet af forordningens artikel 9, stk. 1. Finans Danmark har derfor også med tilfredshed noteret sig, at der foreslås indført en bemyndigelse for vedkommende minister til – efter forhandling med justitsministeren og inden for forordningens rammer – at fastsætte yderligere regler om lovlig behandling af personoplysninger omfattet af forordningens artikel 9, stk. 1. Finans Danmark ser frem til en god og konstruktiv dialog med Erhvervsministeriet og Finanstilsynet om behovet herfor på det finansielle område.

Behandling af betalingsoplysninger

Finansielle virksomheder behandler som led i gennemførelsen af betalingstransaktioner i et vist omfang følsomme oplysninger, der er nødvendige til gennemførelse eller korrektion af en beta-

lingstransaktion. Det kan eksempelvis være i forbindelse med betaling af kontingent til en fagforening, en religiøs sammenslutning eller lignende.

Det fremgår af bemærkningerne til § 125 i den kommende lov om betalinger, at betalingsoplysninger, herunder af potentiel følsom karakter, altid vil kunne behandles, når det er nødvendigt til gennemførelse eller korrektion af en betalingstransaktion, og at der ikke i sådanne tilfælde vil skulle indhentes et udtrykkeligt samtykke fra den betalingsinitierende kunde. Bemærkningerne angår umiddelbart alene samtykkekravet i betalingsloven, men Finans Danmark forudsætter, at der heller ikke gælder et krav om samtykke til disse behandlinger i henhold til persondatareguleringen – hverken efter den nugældende persondatalov eller fremadrettet efter persondataforordningen og databeskyttelsesloven. Da der er tale om en i praksis meget afgørende forudsætning for betalingsområdet, skal Finans Danmark henstille til, at dette tydeliggøres – enten i databeskyttelsesreguleringen eller i den finansielle regulering.

Bioplysninger

Endelig finder Finans Danmark anledning til at gøre opmærksom på den praktisk ofte forekommende situation, at finansielle virksomheder ikke sjældent fra deres kunder modtager mere eller mindre tilfældige (bi)oplysninger, herunder af følsom karakter, der er irrelevante eller omfatter mere end, der er nødvendigt. Problemstillingen gør sig formodentligt tilsvarende gældende i relation til andre virksomheder og offentlige myndigheder.

Finans Danmark er naturligvis opmærksom på princippet om dataminimering i forordningens artikel 5, st. 1, litra c, hvorefter personoplysninger bør være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålene med behandlingen. Det kan imidlertid i praksis vise sig nærved umuligt at udskille og slette oplysninger, der er irrelevante eller omfatter mere end, der er nødvendigt, hvis de eksempelvis indgår som en integreret del af en (elektronisk) korrespondance, der i øvrigt indeholder relevante og nødvendige oplysninger.

Deling af oplysninger i kriminalitetsforebyggende øjemed

Der er efter Finans Danmarks opfattelse et stigende behov for, at finansielle virksomheder kan dele oplysninger ikke bare med politiet og andre myndigheder, men også mellem hinanden, således at kriminelle, der misbruger det finansielle system, kan stoppes hurtigt og effektivt. Behovet stiger i takt med, at der stilles større og større krav til, at finansielle virksomheder påtager sig vigtige samfundsopgaver i forhold til forebyggelse af kriminalitet.

På den baggrund er der efter Finans Danmarks opfattelse behov for større klarhed om, i hvilket omfang private efter den foreslåede bestemmelse i § 8 må behandle og videregive oplysninger om strafbare forhold i kriminalitetsforebyggende øjemed, herunder særligt i hvilket omfang der er adgang til at videregive oplysninger mellem finansielle virksomheder med henblik på at forhindre misbrug af finansielle virksomheder til økonomisk kriminalitet, hvidvask mv.

Indeholder lovforslaget ikke det fornødne hjemmelsgrundlag, bør der – eventuelt i den finansielle lovgivning – tilvejebringes et klart hjemmelsgrundlag selvfølgelig under iagttagelse af de nødvendige retssikkerhedsgarantier.

Det følger af bemærkningerne til lovforslagets § 46, at reglerne om behandling af personoplysninger i forbindelse med tv-overvågning i persondatalovens kapitel 6 a i det kommende følgelovforslag foreslås videreført i tv-overvågningsloven.

Finans Danmark ser frem til muligheden for at afgive bemærkninger hertil og skal i den forbindelse blot bemærke, at det i dag ikke er ganske klart, i hvilket omfang billeder fra overvågningsvideoer kan anvendes internt i eksempelvis et pengeinstituts filialnet i kriminalitetsforebyggende øjemed. Det bør der efter Finans Danmarks opfattelse være mulighed for, ligesom der også på dette praktisk vigtige område bør tilvejebringes det fornødne hjemmelsmæssige grundlag til, at der fremadrettet i højere grad vil kunne deles tv-overvågningsbilleder blandt en gruppe af pengeinstitutter med henblik på kriminalitetsforebyggelse og/eller opklaring.

Personnumre

Finans Danmark noterer sig med tilfredshed, at private efter forslagets § 11 vil have mulighed at behandle oplysninger om personnumre i samme omfang som efter den gældende persondatalov.

Markedsføring

Som anført i forbindelse med bemærkningerne om lovens geografiske område, er Finans Danmark skeptisk i forhold til en national særregel, der stiller danske virksomheder ringere i konkurrence med udenlandske virksomheder. I relation til databeskyttelsesloven knytter dette sig særligt til lovforslagets § 13 om markedsføring, der efter Finans Danmarks opfattelse ikke er i overensstemmelse med regeringens principper for god implementering af EU-regulering, hvilket bør fremgå af lovforslagets sammenfattende skema. I tillæg til spørgsmålet om ulige konkurrence er det endvidere Finans Danmarks opfattelse, at bestemmelsen regulerer et område, som allerede i forordningen er undergivet tilstrækkelig regulering.

Helt konkret i forhold til bemærkningerne til bestemmelsen skal Finans Danmark henstille til, at det kommer til at fremgå udtrykkeligt af bemærkningerne til forslagets § 13, stk. 4, at et samtykke indhentet hos den registrerede af virksomheden går forud for en generel framelding i CPR-registret. Har forbrugeren givet sit udtrykkelige samtykke, skal samtykket på sædvanlig vis tilbagekaldes, før virksomheden skal ophøre med den behandling, som kunden har givet tilladelse til gennem samtykket. Virksomheder, der har et udtrykkeligt samtykke fra den registrerede bør derfor ikke skulle undersøge CPR-registret forud for en videregivelse.

Endelig finder Finans Danmark, at der i relation til reglerne om markedsføring er behov for at klarlægge forholdet mellem kravene i forordningens artikel 21, herunder navnlig artikel 21, stk. 4, og den nye markedsføringslov § 10, stk. 6.

Registreredes rettigheder

De registreredes rettigheder følger af databeskyttelsesforordningen. Udkastet til databeskyttelsesloven indeholder en række bestemmelser om, hvornår disse rettigheder kan begrænses. Der kan således gøres undtagelse fra rettighederne, hvis den registreredes interesse i at få kendskab til en oplysning findes at burde vige for afgørende hensyn til private interesser. På baggrund af bemærkningerne i lovforslaget lægger Finans Danmark til grund, at den eksisterende praksis, hvorefter der ikke gives indsigt i kreditinstitutters interne dokumenter, herunder eksempelvis låneindstillinger, kan fastholdes.

Uafhængige tilsynsmyndigheder

Ifølge lovforslaget skal Datatilsynet føre tilsyn med enhver behandling, der er omfattet af loven, databeskyttelsesforordningen og anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger. Det betyder, at Datatilsynet har tilsynskompetence på alle områder inden for dansk jurisdiktion omfattet af forordningen og lovforslagets anvendelsesområde, herunder områder undergivet dansk særregulering fastast i overensstemmelse med forordningen. Øvrige tilsyn, som eksempelvis Finanstilsynet, der ikke har status som uafhængig tilsynsmyndighed, vil ifølge bemærkningerne til lovforslaget have karakter af supplerende tilsyn i forhold til Datatilsynets generelle tilsyn.

Lov om finansiel virksomhed indeholder i dag særlige behandlingsregler for så vidt angår finansielle virksomheder. Det er Finanstilsynet, der fører tilsyn med overholdelsen af lov om finansiel virksomhed og dermed også med overholdelsen af disse særlige behandlingsregler, og det må derfor være Finanstilsynets tilsyn i den forbindelse, der karakteriseres som "supplerende tilsyn". Efter Finans Danmarks opfattelse står det imidlertid ikke klart, hvad et sådant supplerende tilsyn indebærer i forhold til tilsynsvirksomhed og afgørelseskompetence. Det er afgørende, at der er en klar ansvars- og kompetencefordeling på områder, hvor der potentielt kan være flere kompetente myndigheder – også i lyset af det øgede fokus, der er på databeskyttelsesområdet. Finans Danmark opfordrer til, at Datatilsynet og Finanstilsynet fastlægger klare grænser for ansvars- og kompetencefordelingen, således at det også for de berørte datasubjekter og dataansvarlige står klart, hvordan myndighedsansvaret er placeret.

Efter Finans Danmarks opfattelse er der endvidere behov for at sikre en større grad af ensretning og sammenhæng i forhold til definitioner af begreber, som har rod i databeskyttelsesretten, men som også genfindes i særlovgivningen på eksempelvis det finansielle område. Det er vigtigt, at der er den samme forståelse af de begreber, der anvendes på tværs af de forskellige regelsæt. Som eksempel herpå kan nævnes, at overladelse af data anses som en videregivelse i henhold til den finansielle lovgivning, uagtet at overladelsen blot sker til en databehandler.

Det følger af § 33 i udkastet til lovforslag, at Datatilsynet kan offentliggøre sine afgørelser. Det følger endvidere, at tilsynet er forpligtet til at undlade at offentliggøre oplysninger fra sager, hvis offentlighedens interesse i at få kendskab til et arrangement findes at burde vige for afgørende hensyn til private og offentlige interesser. Det fremgår af bemærkningerne til bestemmelsen, at det i tvivlstilfælde vil være naturligt at indhente en udtalelse herom fra den dataansvarlige, som er part i sagen, og eventuelt tillige fra den registrerede. En sådan udtalelse bør efter Finans Danmarks opfattelse indhentes *hver* gang en afgørelse påtænkes offentliggjort. På den måde sikres det, at Datatilsynet får det bedst mulige grundlag at vurdere offentliggørelsen på. Finans Danmark skal opfordre til, at lovforslaget ændres i overensstemmelse hermed.

Retsmidler, ansvar og sanktioner

Databeskyttelsesforordningen indeholder bestemmelser om, hvordan overtrædelse af forordningen skal sanktioneres. Forordningen angiver herunder maksimale bødeniveauer afhængig af, hvilke bestemmelser der overtrædes. De angivne bødeniveauer er markant højere, end det bødeniveau vi kender fra danske sager vedrørende overtrædelse af persondatareglerne, og Justitsministeriet lægger på den baggrund op til, at der skal ske en væsentlig forøgelse af bødeniveauet for overtrædelse af forordningens bestemmelser i forhold til, hvad overtrædelser af persondataloven i dag takseres til.

Finans Danmark er enig i, at det er vigtigt at sikre en høj grad af beskyttelse af personoplysninger. Vi anerkender derfor også intentionen om at fastsætte et højt bødeniveau for derved at signalere, hvor alvorligt man ser på overtrædelse af persondatareglerne. Samme tendens ses på en række andre områder, herunder også det finansielle område, hvor et udvalg nedsat under Erhvervs- og Vækstministeriet i maj 2016 afgav betænkning om bødesanktioner på det finansielle område, der

resulterede i lovændring om højere bødestraffe[1]. Det er dog samtidig vigtigt at understrege, at bøder blot er én af en række sanktionsmuligheder, som Datatilsynet får med persondataforordningen. Forordningen opererer således også med administrative reaktioner som advarsler, kritik og påbud.

Tilsvarende kendes på det finansielle område, hvor Finanstilsynet kan afgøre sager med påbud og påtaler i tillæg til at søge sagerne afgjort med strafferetlige sanktioner. Disse administrative afgørelsesformer bidrager i vidt omfang til at præcisere og udfylde bestemmelser i den finansielle lovgivning, der indeholder en høj grad af skøn. Finanstilsynet vælger den konkrete reaktionsform ud fra en proportionalitetsbetragtning blandt andet i forhold til overtrædelsens karakter.

I forbindelse med sanktionsudvalgets arbejde blev det eksplicit fremhævet i betænkningen og i det efterfølgende lovforslag, at der med skærpelsen af de strafferetlige sanktioner ikke var tilsigtet en ændring i Finanstilsynets praksis med hensyn til, hvilke tilfælde der søges afgjort med henholdsvis administrative påbud eller påtaler, henholdsvis strafferetlige sanktioner. Finans Danmark skal opfordre til, at samme intention følges i forhold til sager vedrørende databeskyttelsesretten, hvor virksomhedernes adfærd i mange situationer vil være basereret på skønsmæssige vurderinger af, hvordan retsreglerne skal fortolkes under helt konkrete omstændigheder.

I øvrigt

Udkastet til lovforslag indeholder ikke en opgørelse af de økonomiske og administrative konsekvenser for henholdsvis det offentlige og for erhvervslivet.

Implementeringen af et så omfattende regelsæt, som den nye databeskyttelsesregulering er, vil selvsagt være forbundet med betydelige omkostninger for erhvervslivet, også selvom det alene er en videreudvikling af eksisterende regelsæt. Blandt andet nye rettigheder, kravet om en DPO samt kortlægning af datastrømme med henblik på at kunne imødekomme nye tilsynskrav kræver – og vil også fremadrettet kræve – et markant øget ressourceforbrug hos de dataansvarlige. Finans Danmark er bekendt med, at opgørelsen af økonomiske og administrative konsekvenser af lovforslaget ikke vil omfatte alle de omkostninger, der følger direkte af forordningen, men disse er ikke ubetydelige, og opgørelsen heraf bør derfor også indgå som en del af lovgivningsprocessen.

Hvad angår konsekvenserne for det offentlige, vil succesen med nye databeskyttelsesregler til dels være afhængig af, hvor mange ressourcer der vil blive givet til Datatilsynet. Hvis tilsynet skal have mulighed for at gå i dialog med virksomheder, myndigheder og datasubjekter og dermed sikre den bedst mulige forståelse og implementering af reglerne, kræver det, at der afsættes tilstrækkelige ressourcer til opgaven. I modsat fald vil Datatilsynet alene være i stand til at reagere på situationer, frem for at bidrage til at overtrædelser eller misforståelser undgås.
Finans Danmark skal derfor opfordre til, at der afsættes yderligere ressourcer til Datatilsynet for at sikre det bedst mulige tilsyn – ikke blot i implementeringsfasen men også fremadrettet.

[1] Udvalget vedrørende bødesanktioner på det finansielle område (sanktionsudvalget) afgav den 10. maj 2016 betænkning nr. 1561.

Finans Danmark skal afslutningsvis kvittere for, at der tydeligvis er både udført og planlagt et omfattende arbejde i forbindelse med at forberede databeskyttelsesforordningens ikrafttræden. Finans Danmark har i dette høringssvar alene fokuseret på lovforslaget og bemærkningerne hertil. Finans Danmark har modtaget det forslag til følgelov, der skal fremsættes som konsekvens af databeskyttelsesforordningen og databeskyttelsesloven, i høring og ser frem til at komme med bemærkninger hertil.

Justitsministeriet har derudover angivet, at der over det næste halve år vil blive offentliggjort en række vejledninger om forståelsen af forordningen. Finans Danmark ser frem til at blive inddraget i arbejdet med disse vejledninger.

Med venlig hilsen

Helene V. Grønfeldt

Direkte: +45 3370 1060
Mail: hvg@fida.dk

Finans og Leasing
Interesseorganisation for danske finansieringsselskaber

Torveporten 2, 4. sal
DK-2500 Valby
Telefon: +45 27 36 90 19
E-mail: post@finansogleasing.dk
www.finansogleasing.dk
CVR nr. 75 36 12 11

Til Justitsministeriet
Slotholmsgade 10
1216 København K
Att. Nanna Due Binø, Databeskyttelseskontoret
Sagsnr.: 2016-7910-0021

22. august 2017

Tak for det fremsendte høring over udkast til forslag til databeskyttelsesloven - (2016-7910-0021)

Svindelbekæmpelse – bedre mulighed for hindring af svindel

Finans og Leasing har følgende bemærkninger til forslagets § 26 om advarselregistre med henblik på svindelbekæmpelse:

Finans og Leasing vil gerne opfordre til at man følger forordningen og ikke videreindfører det nuværende særlige danske krav om forudgående tilladelse til oprettelse af advarselsregistre.

Der er i dag stort behov for at virksomheder (f.eks. via brancheorganisationer) kan advare hinanden mod svindel herunder forsøg herpå.

Antallet af svindelsager er stigende ligesom hastigheden hvormed de kriminelle går fra én virksomhed til en anden i forsøg på svindel er stigende. Der er således stort behov for at virksomheder kan advare andre virksomheder hurtigst muligt mod *åbenlyse* forsøg på svindel. Her tænkes f.eks. på åbenlyst forfalskede personlige dokumenter såsom årsopgørelser, lønsedler, pas, kørekort mv. Det kan f.eks. være tilfældet hvis der *åbenlyst* er rettet i oplysningerne i dokumenterne eller at der er angivet *åbenlyst* falske oplysninger på disse, og det i øvrigt er relativt simpelt/objektivt muligt at konstatere dette. Det kan f.eks. være en falsk/forkert indkomst eller falsk angivet arbejdsgiver på en lønseddel. Dette kan relativt nemt konstateres som værende falsk ved f.eks. at ringe til oplyst arbejdsgiver, slå arbejdsgiver op i CVR eller lignende. Såfremt en virksomhed i f.eks. en låneproces opdager et sådan åbenlyst forsøg på svindel, og det uden tvivl må kunne lægge til grund, at der ikke var tale om fejlskrift (men bevidst forsøg på svindel), bør denne virksomhed uden problemer kunne advare konkurrenter om at indgå låneaftale med den pågældende person.

Hensynet til beskyttelse af den enkelte (potentielt kriminelle) persons persondatarettigheder, bør efter vores opfattelse i sådanne tilfælde kunne vige for samfundets interesse i at kunne undgå svindel og kriminel aktivitet og således anses for proportionalt.

Som det fremgår af lovforslagets side 216 er der efter databeskyttelsesforordningen netop ikke krav om, at der skal indhentes en tilladelse fra tilsynsmyndighederne inden iværksættelsen af f.eks. advarselsregistre og det følger af forordningens artikel 30, at den dataansvarlige og databehandleren (i stedet) kan/skal føre interne fortegnelser over deres behandling af personoplysninger. Dette ligger i forlængelse af, at forordningen generelt lægger op til at virksomheder der behandler personoplysninger i højere grad selv har ansvaret for lovens overholdelse jf. også Betænkningen s. 450 ”*Ansvarlighed er et gennemgående tema i forordningen, idet den dataansvarlige og i visse*

tilfælde databehandleren, har ansvaret for at forordningens regler efterleves i enhver behandlingsaktivitet".

På trods af at forordningen ikke kræver forudgående tilladelse inden iværksættelse af advarselsregistre, og på trods af at forordningen lægger op til at virksomheder selv udviser ansvarlighed, foreslår Justitsministeriet alligevel, at man opretholder den tidligere anmelderordning til Datatilsynet som betingelse for at kunne oprette et advarselsregister.

Dette begrundes med (jf. artikel 36, stk. 5) at en tilladelsesordningen vil være *"i samfundets interesse" idet der lægges vægt på, at sådanne indgribende former for behandling af personoplysninger vurderes og bedømmes nærmere af Datatilsynet.*"

Endvidere er det Justitsministeriets vurdering, at det er "*påkrævet at fastsætte nærmere regler om registre, der oprettes med henblik på at advare andre imod Forretningsforbindelser, idet det er af meget væsentlig betydning for såvel enkeltpersoner som virksomheder, at registrering i advarselsregistre sker på en saglig og lovlig måde. Ulovlige behandlinger på dette område vil kunne medføre alvorlige skadevirkninger for de involverede parter*."

Finans og Leasing er af den opfattelse, at danske virksomheder – i tråd med forordningens "gennemgående tema" om selvregulering og forordningens manglende behov for at regulere forudgående tilladelser til advarselsregistre – godt selv kan tage ansvar for at oprette et advarselsregister og behandle personoplysningerne heri i overensstemmelse med reglerne.

Vi skal derfor opfordre til at man genovervejer det foreslåede krav om forudgående tilladelse til oprettelse af advarselsregistre således at virksomheder i Danmark nemmere kan imødegå den stigende kriminalitet i form af svindel og bedrag – i samfundet interesse.

Med venlig hilsen

Thomas Benjamin Johansen
Chefkonsulent, Finans og Leasing
Torveporten 2, 4. sal
2500 Valby
tbj@finansogleasing.dk
www.finansogleasing.dk

FA FINANSSEKTORENS ARBEJDSGIVERFORENING

Justitsministeriet
Lovkontoret / Databeskyttelseskontoret
Slotsholmsgade 10
1216 København K

Att. Nanna Due Binø

Sendt pr. e-mail til databeskyttelseskontoret@jm.dk

Den 18. august 2017

DOK. NR.:
FAID-6-50459
SAG. NR:
FAID-6-8019
clr

Bemærkninger til udkast til forslag til databeskyttelsesloven

Finanssektorens Arbejdsgiverforening (FA) har med interesse læst Justitsministeriets forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven), som det er sendt i høring 7. juli 2017.

FA finder overordnet forslaget positivt og vil særligt kvittere for, at det bidrager til at skabe klarhed om rækkevidden af den kommende persondataforordning i forhold til de gældende regler om persondata i databehandling i ansættelsesforhold.

FA har følgende bemærkninger til lovforslaget:

Personoplysninger om afdøde personer
Lovforslaget lader reglerne omfatte personoplysninger om afdøde personer i 10 år efter vedkommendes død. Det fremgår ikke af bemærkningerne til lovforslaget, om dette indebærer, at virksomheder skal opbevare personoplysninger om afdøde medarbejdere i op til 10 år, fx for at kunne besvare henvendelser fra myndigheder eller fra dødsboet.

FA efterlyser en nærmere beskrivelse af, hvorfor der i lovforslaget er valgt en 10 års grænse for behandling af oplysninger om afdøde personer, og hvilken betydning denne grænse forventes at have for databehandling i ansættelsesforhold.

Behandling af personoplysninger i ansættelsesforhold
FA noterer med tilfredshed, at der i forslaget sikres hjemmel til lovlig behandling af personoplysninger før, under og efter ansættelsesforhold i samme omfang som i dag, herunder at forslaget slår helt fast, at samtykke også fremover kan anvendes som lovligt behandlingsgrundlag før, under og efter ansættelse.

Reglerne om behandling af persondata i ansættelsesforhold vil således i høj grad svare til de gældende regler.

FINANSSEKTORENS ARBEJDSGIVERFORENING
AMALIEGADE 7
1256 KØBENHAVN K
T +45 33914700
F +45 33911786
FA@FANET.DK
WWW.FANET.DK

Behandling af personoplysninger i statistisk øjemed
FA noterer også med tilfredshed, at forslaget sikrer, at der ikke sker nogen indskrænkning i forhold til de muligheder, dataansvarlige har for at foretage undersøgelser i statistisk øjemed i den gældende lovgivning.

Databeskyttelsesrådgiveres tavshedspligt
Kravet om tavshedspligt for databeskyttelsesrådgivere er i forslaget knyttet til en selvstændig hjemmel til bødestraf, hvis en databeskyttelsesrådgiver bryder sin tavshedspligt. Det bør tilføjes i bemærkningerne, at arbejdsgiveren, uanset om der pålægges sanktion i form af bøde, vil kunne reagere med ansættelsesretlige sanktioner. Arbejdsgiver vil kunne opsige, eller evt. bortvise, en databeskyttelsesrådgiver, der bryder sin tavshedspligt, uden at komme i konflikt med forordningens beskyttelse af databeskyttelsesrådgivere i artikel 38, stk. 3.

Økonomiske og administrative konsekvenser for det offentlige
FA bemærker, at dette punkt i bemærkningerne til forslaget ikke indeholder nogen tekst.

Forslaget indeholder bestemmelser om tilsynsmyndighedens indretning, der gør det aktuelt at overveje, i hvilket omfang dette har økonomiske eller administrative konsekvenser for det offentlige.

FA opfordrer til, at disse konsekvenser beskrives nærmere i det endelige lovforslag.

Økonomiske og administrative konsekvenser for erhvervslivet
FA bemærker, at også dette punkt i bemærkningerne til forslaget ikke indeholder nogen tekst.

Ændringen af persondataloven sker for at tilpasse loven til persondataforordningen. Dette indebærer bl.a.

- skærpede krav til virksomhedernes systemer
- øgede rettigheder for de registrerede, med deraf følgende administrative belastninger for virksomhederne
- krav om ansættelse af databeskyttelsesrådgivere
- væsentligt skærpede bøder for overtrædelse af reglerne

Forslaget vil derfor have såvel økonomiske som administrative konsekvenser for erhvervslivet, der bør analyseres og tydeliggøres i lovforslaget.

FA opfordrer til, at også disse konsekvenser beskrives nærmere i det endelige lovforslag.

Administrative konsekvenser for borgerne
Det fremgår af det sammenfattende skema, side 252 i forslaget, at forslaget har visse negative administrative konsekvenser for borgerne.

Disse negative administrative konsekvenser for borgerne er ikke nærmere beskrevet, hverken i skemaet eller i afsnit 5, Administrative konsekvenser for borgerne, side 249 i forslaget.

FA opfordrer til, at også disse konsekvenser beskrives nærmere i det endelige lovforslag.

FA har ikke yderligere bemærkninger til lovforslaget i den foreliggende form og henviser i øvrigt til brancheforeningernes høringssvar.

Med venlig hilsen

Claus Ryde
Seniorkonsulent
Direkte: +45 3338 1614

FINANSTILSYNET

N O T A T

Finanstilsynet

30. august 2017

J.nr.
/LEF

Høringssvar til udkast til databeskyttelsesloven

1. Generelle overordnede bemærkninger

Finanstilsynet noterer sig, at det fremgår af lovudkastets § 1, at loven supplerer og gennemfører persondataforordningen. Da der er tale om en forordning, har persondataforordningen direkte virkning i Danmark, som det tillige fremgår af de almindelige bemærkninger til lovudkastet, jf. s. 150. Finanstilsynet er derfor af den opfattelse, at det alene bør fremgå af § 1, at loven supplerer forordningen.

2. Forholdet mellem databeskyttelsesloven og den finansielle lovgivning (særregler)

Finanstilsynet noterer sig, at det af lovudkastets § 1, stk. 3, fremgår, at regler om behandling af personoplysninger i anden lovgivning, går forud for reglerne i databeskyttelsesloven. I forbindelse med udarbejdelse af Justitsministeriets betænkning om persondataforordningen har Finanstilsynet fået bekræftet, at det er muligt at opretholde bl.a. de gældende regler om finansielle virksomheders videregivelse og udnyttelse af fortrolige oplysninger i kapitel 9 i lov om finansiel virksomhed (herefter kaldet FIL).

Det er Finanstilsynets opfattelse, at det dermed betyder, at reglerne i kapitel 9 i FIL vil gå forud for reglerne i den nye databeskyttelseslov, herunder også i forhold til den foreslåede § 2, stk. 5, om at databeskyttelsesloven og forordningen finder anvendelse på afdøde personers oplysninger i 10 år efter vedkommendes død. Dette er særligt vigtigt, da videregivelsesreglerne i kapitel 9 i FIL ikke har en tidsmæssig begrænsning, og derfor beskytter kunders oplysninger, selvom de har været døde i mere end 10 år.

3. Tilsynskompetence

Finanstilsynet finder, at formuleringen og bemærkningerne til forslagets § 27, stk. 1, om Datatilsynets tilsynskompetence ikke er tilstrækkeligt klare med hensyn til, hvem der er tilsynsmyndighed i forhold til reglerne om behandling

af persondata i den finansielle lovgivning, herunder reglerne i kapitel 9 i FIL, når den nye databeskyttelseslov træder i kraft.

I dag går reglerne i kapitel 9 i FIL, forud for reglerne i persondataloven, jf. § 2, stk. 1, i persondataloven, og Finanstilsynet er tilsynsmyndighed i forhold til kapitel 9 i FIL om finansielle virksomheders videregivelse og udnyttelse af fortrolige oplysninger. I praksis, har Datatilsynet oversendt klager over finansielle virksomheders videregivelse af personoplysninger til afgørelse i Finanstilsynet.

Det fremgår af lovforslagets almindelige bemærkninger s. 226, at Justitsministeriet i forhold til Datatilsynets organisation i vidt omfang foreslår en videreførelse af den gældende ordning. Det fremgår videre, at dette indebærer, at Datatilsynet har tilsynskompetence på alle områder inden for dansk jurisdiktion omfattet af forordningen og lovforslagets anvendelsesområde, herunder områder undergivet *dansk særregulering fastsat i overensstemmelse med forordningen (*Finanstilsynets fremhævelse). Sidst fremgår det, at øvrige tilsyn, såsom Finanstilsynet, der ikke har status af uafhængige tilsynsmyndigheder vil have karakter af *supplerende tilsyn* (Finanstilsynets fremhævelse) i forhold til Datatilsynets generelle tilsyn.

Det er ikke i bemærkningerne forklaret yderligere, hvad der forstås ved *supplerende tilsyn.* Bemærkningerne giver derfor indtryk af, at Datatilsynet fremover vil være den kompetente tilsynsmyndighed både i forhold til databeskyttelsesloven, men også i forhold til nationale særregler om behandling af personoplysninger, herunder i forhold til lov om finansiel virksomhed.

På baggrund af Justitsministeriets betænkning og de løbende drøftelser, som Finanstilsynet har haft med Erhvervsministeriets departement og Justitsministeriet, har meldingen fra Justitsministeriet været, at den danske særlovgivning vil kunne bestå ved siden af Persondataforordningen og at Finanstilsynet vil kunne fortsætte med at være tilsynsmyndighed for så vidt angår kapitel 9 i FIL, ligesom det er i dag.

Finanstilsynet foreslår derfor, at det tydeliggøres i bemærkningerne, at Finanstilsynet, også efter den nye databeskyttelseslov og persondataforordningen træder i kraft, vil fortsætte med at være tilsynsmyndighed for så vidt angår regler om behandling af persondata i den finansielle regulering, herunder bl.a. lov om finansiel virksomhed, mens Datatilsynet er den overordnede kompetente myndighed i forhold til forordningen og særreguleringen. Finanstilsynet foreslår endvidere, at der i bemærkningerne indsættes eksempler på, hvordan forholdet mellem Datatilsynet, som uafhængig tilsynsmyndighed, og et supplerende tilsyn, som f.eks. Finanstilsynet, ser ud i de sager, hvor behandlingen af personoplysninger fremgår af særlovgivningen, herunder om en kunde kan klage over en overtrædelse af videregivelsesreglerne i den finansielle

lovgivning til Datatilsynet, og at Datatilsynet vil være kompetent til at behandle denne klage.

Finanstilsynet er opmærksom på, at det kan medføre enkelte tilfælde, hvor en behandling af personoplysninger bliver underlagt en form for dobbelttilsyn. På den baggrund – og også set i lyset af den såkaldte Se og Hør-sag – vil Finanstilsynet snarest muligt tage kontakt til Datatilsynet med henblik på at fastsætte rammerne for det fremtidige tilsyn i forhold til de finansielle virksomheder, f.eks. via en samarbejdsaftale.

SAMMEN
GØR VI FORSKELLEN

Justitsministeriet
Slotsholmsgade 10
1216 København K
Sendt via e-mail: databeskyttelseskontoret@jm.dk

Høringssvar til udkast til forslag om databeskyttelsesloven

Med henvisning til Justitsministeriets brev af 7. juli 2017 om høring over udkast til forslag til databeskyttelsesloven kan FOA - Fag og Arbejde oplyse, at forbundet tilslutter sig indholdet i det af LO, FTF og AC afgivne høringssvar, dateret den 22. august 2017.

Med venlig hilsen

Lotte Salenborn
Chef for FOA Overenskomst

Dato:
22. august 2017

Sagsnr.:
17/178008

Ref.:
ssg001

FOA

Staunings Plads 1-3
1790 København V

Tlf.:
+45 46 97 26 26

Fax:
+45 46 97 23 00

Kontonr.:
5301-0476807

Mail:
foa@foa.dk
a-kassen@foa.dk

www.foa.dk

FORBRUGEROMBUDSMANDEN

Justitsministeriet
Lovafdelingen
Slotholmen 10
1216 København K

Att. Nina Due Binø

Dato: 20. september 2017

Sag: FO-17/10307-2

Sagsbehandler: /JOT
Direkte tlf.: +45 41 71 51 36

FORBRUGEROMBUDSMANDEN
Carl Jacobsens Vej 35
2500 Valby

Tlf. 41 71 51 51
Fax 41 71 51 61
CVR-nr. 10 29 48 19
EAN-nr. 5798000018006
forbrugerombudsmanden@kfst.dk
www.forbrugerombudsmanden.dk

ERHVERVSMINISTERIET

Forbrugerombudsmandens høringssvar over udkast til forslag til følgelov til databeskyttelsesloven

Forbrugerombudsmandens høringssvar angår navnlig spørgsmålet om, i hvilket omfang lovforslagene om databeskyttelse vil medføre ændringer i den nuværende tilsynsstruktur og om dette i givet fald vil være hensigtsmæssigt.

Resume

- Forbrugerombudsmanden har antaget, at den gældende tilsynsstruktur videreføres. Forbrugerombudsmanden har i så fald ingen substantielle bemærkninger til lovforslagene. Der henvises til afsnit 2 og 5 neden for.

- Forbrugerombudsmanden har dog erfaret, at den foreslåede tilsynsbestemmelse i § 27 i udkastet til ny databeskyttelseslov har givet anledning til tvivl om, hvorvidt lovforslaget vil medføre en ny tilsynsstruktur.

  Hvis der med lovforslagene er tilsigtet en tilsynsordning, hvor Datatilsynet skal varetage tilsynet med alle lovbestemmelser i særlovgivningen, *som afviger* fra databeskyttelsesloven f.eks. ved at forbyde eller på anden måde begrænse anvendelsen af data på særlige områder, vil det indebære betydelige ændringer af den nuværende tilsynsordning.

- En sådan ændring af den gældende tilsynsordning må efter Forbrugerombudsmandens opfattelse forudsætte tydelig lovhjemmel og ville rejse en række vanskelige spørgsmål, som ikke er adresseret i lovforslagene og allerede derfor ville kunne give anledning til betydelig retsusikkerhed. Der henvises til afsnit 3 og 4 nedenfor.

Forbrugerombudsmandens høringssvar følger neden for i sin helhed.

1. Udkast til en ny databeskyttelseslov og følgelovforslaget

Det fremgår af bemærkningerne til følgelovforslagets § 17, nr. 3 og 4 om konsekvensændringer i betalingstjenesteloven,

> *at forordningen således indebærer, at Datatilsynet har tilsynskompetence på alle områder inden for dansk jurisdiktion omfattet af forordningens anvendelsesområde, herunder områder undergivet dansk særregulering fastsat i overensstemmelse med forordningen.*

I overensstemmelse hermed foreslås i databeskyttelseslovforslagets § 27, stk. 1, at Datatilsynet skal føre tilsyn med anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler. I bemærkningerne til denne bestemmelse er anført, at det i vidt omfang er en videreførelse af den gældende ordning, og at

> *Øvrige tilsyn, såsom Finanstilsynet og Forbrugerombudsmanden, der ikke har status af uafhængige tilsynsmyndigheder, vil have karakter af supplerende tilsyn i forhold til Datatilsynets generelle tilsyn.*

Forbrugerombudsmanden skal gøre opmærksom på, at Forbrugerombudsmanden *er* en uafhængig myndighed, hvis afgørelser ikke kan indbringes for anden administrativ myndighed, jf. markedsføringslovens § 25, stk. 3 og 4, og betalingslovens § 144, stk. 5. Forbrugerombudsmanden skal henvise til sit høringssvar af 21. august 2017 til udkastet til en ny databeskyttelseslov.

Spørgsmålet om tilsynet med overholdelse af anden særlovgivning end databeskyttelsesloven er ikke nærmere uddybet i lovforslagene.

2. Videreførelse af den nuværende tilsynsordning

Da Justitsministeriet har tilkendegivet i lovforslagene, at den gældende tilsynsordning i vidt omfang videreføres, har Forbrugerombudsmanden forstået lovforslagene således, at Datatilsynet fortsat skal føre tilsyn med databeskyttelsesregler i anden særlovgivning, *i det omfang* særlovgivningen henviser til reglerne i databeskyttelsesloven.

Forbrugerombudsmanden har heller ikke kunnet udlede af databeskyttelsesforordningen, at den ledende databeskyttelsestilsynsmyndighed skal tillægges tilsynskompetencen med særlovgivning, der er fastsat i overensstemmelse med forordningen.

Forbrugerombudsmanden har derfor ikke kommenteret dette spørgsmål i sit høringssvar til udkastet til en ny databeskyttelseslov.

3. Kommentarer til en eventuel ændring af tilsynsordningen

Forbrugerombudsmanden har dog nu erfaret, at den foreslåede tilsynsbestemmelse i § 27 i udkastet til ny databeskyttelseslov har givet anledning til tvivl om, hvorvidt lovforslaget vil medføre en anden tilsynsstruktur end den nuværende.

Hvis det er hensigten med lovforslagene, at Datatilsynet fremover skal være tilsynsmyndighed med alle lovbestemmelser i særlovgivningen, *som afviger* fra databeskyttelsesloven f.eks. ved at forbyde eller på anden måde begrænse anvendelsen af data på særlige områder, vil det indebære betydelige ændringer af den nuværende tilsynsordning.

En sådan ændring af den gældende tilsynsordning må efter Forbrugerombudsmandens opfattelse forudsætte tydelig lovhjemmel og rejser en række vanskelige spørgsmål, som ikke er adresseret i lovforslagene:

- Hvis Datatilsynet fremover skal varetage tilsynet med anden lovgivning end databeskyttelsesloven og forordningen, bør spørgsmålet om, hvilken tilsynsmyndighed der har *det primære ansvar* for at føre tilsyn med bestemmelser, som afviger fra databeskyttelsesloven ved at forbyde eller på anden måde begrænse anvendelsen af data på særlige områder, adresseres. Efter den gældende særlovgivning er det spørgsmål adresseret ved at udpege en tilsynsmyndighed i særlovgivningen.

- Det bør fastlægges, hvornår henholdsvis Datatilsynet og de "supplerende tilsynsmyndigheder" har kompetence til at træffe afgørelser, om der skal være dobbelttilsyn, og i så fald hvilke konsekvenser det har for Datatilsynets kompetence til at træffe afgørelse, når der allerede er truffet afgørelse af en anden tilsynsmyndighed i en sag.

- Hvis Datatilsynet får kompetence i sager, hvor en anden tilsynsmyndighed allerede har truffet afgørelse, opstår spørgsmålet om, hvilken retsvirkning Datatilsynets afgørelse har, herunder når den første afgørelse er truffet af uafhængige tilsynsmyndigheder. Spørgsmålet om retsvirkningerne af Datatilsynets afgørelser i en sådan situation er ikke omtalt i lovforslaget.

Efter Forbrugerombudsmandens opfattelse vil disse spørgsmål kunne give anledning til betydelig retsusikkerhed.

Om en ændring af tilsynsstrukturen ville være hensigtsmæssig, er heller ikke adresseret i lovforslagene eller i betænkning nr. 1565, som ligger til

grund for lovforslagene. Forbrugerombudsmanden tillader sig at stille spørgsmål ved, om en centralisering af tilsynsopgaven med al særregulering om behandling af personoplysninger vil være hensigtsmæssig i lyset af den betydning som behandling af persondata må antages at få i fremtiden. Afgørende for et effektivt tilsyn er, at tilsynsmyndigheder har indsigt i den aktivitet, der reguleres i særlovgivningen.

4. Forbrugerombudsmandens tilsyn med betalingsloven

Forbrugerombudsmanden fører bl.a. tilsyn med, at virksomheder overholder de forbrugerbeskyttende regler i den gældende betalingstjenestelov og kommende betalingslov, herunder betalingslovens § 124 og § 125[1]. Disse bestemmelser fastsætter særregulering ved behandling af personoplysninger ved udbuddet af betalingstjenester.

Således som databeskyttelseslovforslagene er formuleret, har Forbrugerombudsmanden antaget, at lovforslagene ikke indebærer ændringer i den nuværende tilsynsordning, hvor Datatilsynet er den primære tilsynsmyndighed for så vidt angår spørgsmålet om, hvorvidt persondatalovens regler overholdes. Betalingstjenesteloven og den kommende betalingslov indeholder begge henvisninger til persondatalovens bestemmelser. Forbrugerombudsmanden varetager tilsynet med overholdelsen af de videregående særregler om behandling af persondata ved brug af betalingsmidler.

Hvis hensigten er, at Datatilsynet fremover skal være tilsynsmyndighed også for så vidt angår de særregler, hvor tilsynet er tillagt Forbrugerombudsmanden, jf. betalingslovens § 144, rejser det en række spørgsmål, som ikke er adresseret, herunder om Forbrugerombudsmandens uafhængige tilsyn bliver et supplerende tilsyn ift. Datatilsynets tilsyn. Retsvirkningerne heraf er heller ikke berørt. Som uafhængig tilsynsmyndighed kan Forbrugerombudsmandens afgørelser ikke indbringes for anden administrativ myndighed, jf. betalingslovens § 144, stk. 5

Under alle omstændigheder bør fordelingen af tilsynskompetence klart adresseres og begrundes i lovforslagene, hvis lovforslagene tilsigter at medføre ændringer af tilsynskompetencen.

[1] Betalingslovens § 144. Betalingsloven træder i kraft den 1. januar 2018 og afløser herved den nugældende betalingstjenestelov.

5. Datatilsynets samarbejde med udenlandske myndigheder

Det fremgår af bemærkningerne til følgelovforslagets § 17, nr. 3 og 4, at Datatilsynet kan indgå i dialog med Finanstilsynet i forbindelse med Finanstilsynets samarbejde med udenlandske myndigheder.

Det bør samtidig fremgå af bemærkningerne til følgelovforslagets § 17, nr. 3 og 4, at Datatilsynet kan indgå i dialog med Forbrugerombudsmanden i forbindelse med Datatilsynets samarbejde med udenlandske myndigheder, da følgelovforslagets § 17, nr. 4, angår samarbejdet mellem Datatilsynet, Forbrugerombudsmanden og udenlandske myndigheder, og da Forbrugerombudsmanden som nævnt ligeledes fører tilsyn med bestemmelser i betalingsloven.

6. Brug af persondata i markedsføring

Forbrugerombudsmanden tillader sig endelig at gøre opmærksom på, at Forbrugerombudsmanden i kraft af bestemmelsen om god markedsføringsskik i markedsføringslovens § 3, stk. 1, og bestemmelsen om god erhvervsskik i markedsføringslovens § 4 kan inddrage spørgsmål om brug af persondata i markedsføring.

Erhvervsdrivende behandler i stigende grad forbrugeres persondata i markedsføringsøjemed, fx ved aftaleindgåelse eller ved udsendelse af elektronisk markedsføring, og forbrugere "betaler" ligeledes i stigende omfang for ydelser ved afgivelse af personoplysninger.

Forbrugerombudsmanden tillægger det derfor stor betydning for effektiviteten af sit fremtidige tilsyn med erhvervslivets overholdelse af den forbrugerbeskyttende lovgivning, at Forbrugerombudsmanden kan inddrage spørgsmål om brug af persondata. I modsat fald ville Forbrugerombudsmanden ikke kunne vurdere væsentlige problemstillinger vedrørende erhvervsvirksomheders markedsføring i fremtiden.

Forbrugerombudsmanden skal endelig beklage, at høringssvaret ikke er afgivet inden for den fastsatte frist.

Med venlig hilsen

Christina Toftegaard Nielsen
Forbrugerombudsmand

FORBRUGEROMBUDSMANDEN

Justitsministeriet
Lovafdelingen
Slotsholmsgade 10
1216 København K

Dato: 21. august 2017

Sag: FO-17/08559-3

Sagsbehandler: /JOT
Direkte tlf.: +45 41 71 51 36

FORBRUGEROMBUDSMANDEN
Carl Jacobsens Vej 35
2500 Valby

Tlf. 41 71 51 51
Fax 41 71 51 61
CVR-nr. 10 29 48 19
EAN-nr. 5798000018006
forbrugerombudsmanden@kfst.dk
www.forbrugerombudsmanden.dk

ERHVERVSMINISTERIET

Høring over udkast til databeskyttelsesloven

Forbrugerombudsmanden skal herved fremkomme med følgende bemærkninger til forslag til databeskyttelsesloven, som er sendt i høring den 7. juli 2017.

Forbrugerombudsmanden noterer sig med tilfredshed, at databeskyttelsesforordningens samtykkekrav, herunder at afgivelse af samtykke skal være frivilligt og informeret, i vidt omfang ses at være i overensstemmelse med praksis efter markedsføringsloven om samtykke til elektronisk markedsføring.

Forbrugerombudsmanden skal endvidere gøre opmærksom på, at det ikke er korrekt som anført i lovforslaget s. 226, at Forbrugerombudsmanden ikke har status som uafhængig tilsynsmyndighed. Der henvises til markedsføringslovens § 25.

Med venlig hilsen
På Forbrugerombudsmandens vegne

Louise Christophersen
Kontorchef

Fiolstræde 17 B, Postboks 2188, 1017 København K
T: +45 7741 7741, F: +45 7741 7742, fbr@fbr.dk, taenk.dk

Justitsministeriet
Sendt pr. e-mail til
databeskyttelseskontoret@jm.dk

22-08-2017
Dok. 168771/ah

Høringssvar til forslag til databeskyttelsesloven

Med henvisning til Justitsministeriets e-mail af 7. juli 2017 skal Forbrugerrådet Tænk hermed fremkomme med bemærkninger til forslag om lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven). Da Justitsministeriets betænkning nr. 1565 udgør et væsentligt fortolkningsbidrag til forordningen, vil Forbrugerrådet Tænk også kommentere kort på den.

Indledningsvist vil Forbrugerrådet Tænk takke for at vi, sammen med Institut for Menneskerettigheder på en række møder, har haft mulighed for at drøfte udvalgte afsnit i databeskyttelsesforordningen med Justitsministeriet. Desuden bemærkes, at Justitsministeriet har udarbejdet en meget grundig og omfattende betænkning, men der er fortsat et stort behov for, at Justitsministeriet og Datatilsynet udarbejder et antal vejledninger, som bør være konkrete og praktisk anvendelige samt sikre en bred forståelse for den ny forordning.

Baggrund

Behov for nye databeskyttelsesregler

Forbrugerrådet Tænk ser digitaliseringen som en stor gevinst for forbrugerne og for vores samfund generelt. Udviklingen har medført, at personlige oplysninger indsamles og udnyttes i et hidtil uset omfang af både myndigheder og private virksomheder. Dette generer viden, bedre service og smarte digitale tjenester, men udfordrer i høj grad også den enkelte forbrugers ret til privatliv og kontrol af oplysninger, samt it-sikkerheden generelt.

En stærk og effektiv databeskyttelseslov er derfor et vigtigt fundament fremover. Vi finder samtidig, at man fra politisk side bør understøtte de nye regler med indsatser, der sikrer en bred bevidsthed om regler, rettigheder og pligter, nye investeringer i privatlivsfremmende teknologi samt øget gennemsigtighed på markedet for digitale tjenester og produkter. Det vil styrke forbrugernes tryghed, som er en afgørende forudsætning for øget innovation og vækst herhjemme.

Bemærkninger til betænkning 1565 om databeskyttelsesforordningen

Nye rettigheder og krav skal ikke "tales ned"

Forbrugerrådet Tænk finder, at der er vigtige nyskabelser i forordningen, som samlet set øger forbrugeres mulighed for at kontrollere oplysninger på nettet og fornyer kravene til virksomhedernes it-sikkerhed og databeskyttelse. Også det styrkede samarbejde på tværs af myndighederne i EU, samt de nye sanktionsmuligheder, kan forbedre håndhævelsen og respekten for reglerne.

Justitsministeriet og Datatilsynet nedtoner i deres formidling af reglerne, at der er nye, vigtige krav på vej, som virksomheder og myndigheder skal forholde sig aktivt til. Vi er uenige i, at der er grundlag for denne formidling. Når myndighederne gang på gang udtaler, at reglerne i vidt omfang svarer til de eksisterende regler, kan man frygte, at virksomheder og myndigheder ikke vil tage de nye regler alvorligt, hvormed beskyttelsesniveauet ikke løftes i tråd med forordningens formål.

Forbrugerrådet
Tænk

Også i betænkningen ses denne tendens, idet forordningens nyskabelser kun fremgår i bisætninger undervejs, ligesom der generelt udvises stor forsigtighed med at indfortolke en bedre forbrugerbeskyttelse eller nye it-sikkerhedskrav i reglerne fra EU. I det følgende vil vi gerne fremhæve tre eksempler herpå.

Privacy by Design krav er et helt afgørende nyt krav

Særligt i forhold til databeskyttelsesforordningens artikel 25 om databeskyttelse gennem design og standardindstillinger finder Forbrugerrådet Tænk, at justitsministeriets fortolkning er for snæver.

Justitsministeriet konkluderer således, at principperne er nyskabelser, men må fortolkes i overensstemmelse med 1995-direktivets artikel 17 samt praksis, hvorefter dataansvarlige forpligtes til at gennemføre "passende og tekniske og organisatoriske foranstaltninger" til at beskytte personoplysninger.

Vi finder derimod, at artikel 25 bør fortolkes i overensstemmelse med artikel 29- gruppens udtalelser om Privacy by Design og de oprindelige canadiske principper, som ikke begrænser sig til kun at omhandle "tekniske og organisatoriske krav". Privacy by design og by default forstås bredere, idet gennemsigtighed, dataminimering og forbrugerkontrol med oplysninger også indgår i de canadiske principper.

Retten til at blive glemt styrker forbrugernes retsstilling

Uanset at princippet om retten til at blive glemt ikke er en ubetinget ret og selvom forbrugere allerede i dag indenfor visse betingelser har mulighed for at få berigtiget, slettet eller blokeret oplysninger, finder vi også her, at justitsministeriet fortolker reglen for snævert, når de konkluderer, at artikel 17 overordnet set er en videreførelse af gældende dansk ret.

Vi mener derimod, at der er tale om en styrkelse af forbrugernes retstilling og henviser til, at det i præamblen fastslås, at reglen især er tiltænkt forbrugere, der som børn har givet samtykke til dataindsamling, men som ikke har været bekendt med risiciene og derfor senere ønsker at få fjernet oplysninger på nettet.

Dertil kommer, at forordningen indeholder en pligt til at slette indsamlede oplysninger, hvis forbrugeren gør brug af sin ret til at tilbagekalde sit samtykke. I modsætning til i dag, hvor en tilbagekaldelse alene forpligter den dataansvarlige til fremadrettet at ophøre med at behandle vedkommendes oplysninger. Endelig er det en stramning, at det fremover er forbrugeren og ikke virksomheden, der beslutter, hvorvidt oplysningerne skal slettes eller blot berigtiges eller blokeres.

Dog er retten til at blive slettet i forordningen fulgt op af betydelige undtagelser. Det gælder særligt forordningens artikel 17, stk. 3 litra b, som reelt undtager offentlige myndigheder fra reglerne om sletning. Forbrugerrådet Tænk skal henlede opmærksomheden på, at journalføringsbekendtgørelsen på sundhedsområdet udelukker patienter fra ret til at få deres oplysninger slettet. Dette gælder også åbenbart forkerte oplysninger, som ikke er lagt til grund for beslutning om behandling. Forbrugerrådet Tænk skal opfordre til at fjerne denne særregel i forbindelse med databeskyttelsesforordningens ikrafttræden.

Forbud mod automatisk profilering kan få stor betydning

Forbrugerrådet Tænk finder også, at det er en vigtig nyskabelse, at forbrugere, der bliver profileret på nettet, typisk via tracking, ikke kan gøres til genstand for automatiske, individuelle afgørelser uden udtrykkeligt samtykke. Hermed tænkes på computeralgoritmer, der uden menneskelig indblanding analyserer forbrugernes helbred, økonomi, præferencer, arbejdsindsats eller bevægelser, og på den baggrund træffer en afgørelse, som fx et afslag på et lån, som påvirker forbrugeren betydeligt. Forbrugere har efter nuværende regelsæt også ret til at sige fra overfor automatisk behandlinger, men det er nyt, at brug af algoritmer også er udtrykkeligt omfattet bestemmelsen.

Bemærkninger til lovforslaget om den supplerende databeskyttelseslov

§ 3 stk. 2-4 – Undtagelser til loven og databeskyttelsesforordningens anvendelsesområde
Forbrugerrådet Tænk finder, at undtagelsen i stk. 2 om at reglerne ikke finder anvendelse på den behandling af personoplysninger, som udføres for eller af politiets og forsvarets efterretningstjenester er for bred. Det skyldes, at selve institutionerne undtages reglerne fuldstændigt og ikke blot de konkrete aktiviteter indenfor deres virke, som fordrer, at databeskyttelsesreglerne ikke skal finde anvendelse.

I forhold til stk. 3, mener vi det er uklart, hvad der præcis ligger i formuleringen Folketingets "parlamentariske arbejde", og som medfører, at reglerne ikke finder anvendelse. Det bør derfor i bemærkninger klart afgrænses og præciseres, hvad der ligger i betydningen "parlamentarisk arbejde".

Endelig finder vi at stk. 4, hvorefter behandlinger omfattet lov om massemediers informationsdatabaser undtages loven, er meget bredt formuleret, og vi skal opfordre til, at databeskyttelsesloven ikke udvider området i forhold til praksis i dag.

§ 4 – Lovens geografiske område
Forbrugerrådet Tænk støtter § 4, stk. 1, hvorefter loven finder anvendelse for dataansvarlige og databehandlere etableret i Danmark. Og ligeledes finder vi, at stk. 3 om, at loven også gælder under visse betingelser, når danske forbrugere handler eller søger information hos virksomheder, som er etableret udenfor EU, er vigtig og lægger sig op af praksis i dag.

§ 5 – Grundreglen om formålsbestemthed
Forbrugerrådet Tænk er grundlæggende imod, at offentlige myndigheder kan undtages grundprincippet om formålsbestemthed, som beskytter forbrugerne mod, at indhentede oplysninger på et senere tidspunkt kan blive videreanvendt til andre formål uden samtykke.
Uanset at det sker i et eller andet omfang efter persondataloven i dag, er vi stærkt betænkelige ved at forslaget i § 5, stk. 3 giver ministre en generel hjemmel til på bekendtgørelsesniveau at fastsætte regler, der undertager myndighederne fra dette grundprincip.

Samtidig må der henvises til § 23, som er særlig problematisk - og som der henvises til i § 5, stk. 3 – fordi den lægger op til, at man fra dansk side bestemmer, at forbrugerne udelukkes fra at få information om, at denne viderebehandling udenom formålet finder sted. Uanset at dette allerede følger af reglerne i dag, og kun gælder under særlige skrappe betingelser som statens sikkerhed mv., støtter vi ikke reglen. Vi mener den skrider grundlæggende imod princippet om transparens og forværrer forbrugernes mulighed for at have kontrol over personlige oplysninger, som den ny forordning netop har til formål at styrke.

§ 6 – Behandling af oplysninger, herunder om børn
Forbrugerrådet Tænk kan tilslutte sig reglen i § 6, stk. 3 om, at behandling af personoplysninger om et barn er lovlig, hvis barnet er mindst 13 år og at forældresamtykke skal indhentes, såfremt barnet er under 13 år jf. forordningens artikel 8.

I den forbindelse skal Forbrugerrådet Tænk opfordre justitsministeriet til at udarbejde en vejledning om, hvordan denne aldersgrænse sikres i praksis, når dataindsamlingen foregår på nettet, herunder også, hvordan man indhenter forældresamtykke for børn under 13 år.

§ 7 - Behandling af følsomme oplysninger
Forbrugerrådet kan ikke støtte forslagets § 7, stk. 4 som undtager offentlige myndigheder fra at søge

tilsynsmyndigheden (Datatilsynet) om tilladelse til at behandle følsomme oplysninger uden samtykke af hensyn til væsentlige samfundsinteresser. Med forslaget bliver det op til den dataansvarlige selv at fortage denne interesseafvejning. Efter den nugældende persondatalov gælder der ikke en undtagelse for offentlige myndigheder, i det de på linje med private virksomheder skal søge tilladelse inden behandlingen. Vi mener forslaget giver forbrugerne en markant forringelse af deres retssikkerhed.

§ 11 – Behandling af personnummer/cpr-numre

Forbrugerrådet Tænk er imod den praksis, som har udviklet sig indenfor private virksomheders brug af cpr-numre. Med lovforslaget ønsker justitsministeriet at ophøje praksis til lov, hvilket vi ikke kan støtte. Vi finder, at virksomheders brug af cpr-numre skal begrænses til tilfælde, hvor tilladelsen specifikt følger af lov, hvorfor vi ønsker, at stk. 2, nr. 2 om samtykke og stk. 2, nr. 3 om "naturligt led i drift" skal slettes af forslaget.

Vi oplever, at forbrugere i dag "tvinges" til at afgive samtykke, som betingelse for at opnå en given tjeneste eller ydelse, når virksomheden ønsker at indsamle cpr-nummer. Et samtykke på dette område har ikke karakter af frivillighed i tråd med samtykkereglen i § 7, når forbrugeren ikke har en reel valgfrihed.

I forhold til stk. 2, nr. 3 finder vi, at hensynet til at lette virksomhedens drift ikke bør begrunde, at forbrugerne forpligtes til at oplyse cpr-nummer. Risikoen for identitetstyveri og datamisbrug i øvrigt samt det forhold, at virksomheder nemt bør kunne verificere kunders identitet på andre og mere sikre måder, gør at vi forslår en stramning af reglerne.

§ 13 – Målrettet markedsføring

Forbrugerrådet Tænk støtter en videreførelse af de nuværende regler om, at virksomheder ikke må videregive oplysninger om en forbruger til en anden virksomhed, medmindre forbrugeren har givet sit udtrykkelige samtykke. Og ligeledes, at de oplysninger om generelle kundeoplysninger, hvor der ikke kræves samtykke, ikke må omhandle følsomme oplysninger efter artikel 9 eller oplysninger om børn under 13 år, medmindre forældrene har givet samtykke jf. artikel 8.

Vi mener imidlertid, at det er vigtigt, taget den digitale udvikling og nye markedsføringsmetoder i betragtning, at § 13, stk. 1-3 også finder anvendelse på virksomheder, som lever af at indsamle og videregive digitale oplysninger som indsamles på internettet, via mobiltelefonen eller via apps. Her tænkes på de såkaldte "databrockere", som ikke bør kunne omgå reglerne om udtrykkeligt samtykke, blot fordi de agerer og indsamler oplysninger digitalt. Af lovforslagets nuværende ordlyd, er det uklart, hvorvidt disse nye markedsføringsmetoder, hvor data deles mellem virksomheder digitalt, er omfattet.

§23 – Undtagelse fra oplysningspligten

Som nævnt under § 5, stk. 3 kan Forbrugerrådet Tænk ikke støtte forslaget om, at oplysningspligten, som er en væsentlig rettighed efter forordningen, ikke finder anvendelse i de tilfælde, hvor offentlige myndigheder viderebehandler personoplysninger til nye formål uden samtykke. Forbrugerrådet Tænk er skeptisk overfor, at offentlige myndigheder på bekendtgørelsesniveau kan gives en særlig adgang til at viderebehandle oplysninger udenfor formålet og uden at oplyse forbrugeren herom. Vi kan ikke støtte, at Danmark udnytter muligheden for særregler her, da det undergraver gennemsigtigheden for myndighedernes databrug og forringer forbrugernes kontrol med egne oplysninger.

§ 15-23 – Kreditoplysninger

Forbrugerrådet Tænk støtter opretholdelse af de danske særregler om videregivelse af oplysninger til kreditoplysningsbureauer samt kravene til kreditoplysningsbureauers behandling af oplysninger om økonomisk solidaritet og kreditværdighed. Også her er det vigtigt at være opmærksomhed på, at reglerne også bør finde anvendelse for kreditoplysningsbureauer, som eventuelt kun agerer på nettet. I den forbindelse skal vi foreslå, at i § 21, stk. 4 suppleres med et klart forbud mod private eller offentlige virksomheders brug af "kreditscore"-redskaber på individuelt niveau (hvilket er en udbredt praksis i visse andre lande både inde - og udenfor EU).

§ 24 – Databeskyttelsesrådgivere

Forbrugerrådet Tænk finder, at forordningens artikel 37, som stiller krav om, at offentlige og private virksomheder i visse tilfælde skal udpege databeskyttelsesrådgivere, er en vigtig nyskabelse i forordningen. Databeskyttelsesrådgivere kan sikre et øget fokus på databeskyttelse og it-sikkerhed hos den virksomhed, hvor vedkommende er placeret, og indirekte bistå Datatilsynet i forhold til rådgivning om emnet.

I betænkningen konkluderer Justitsministeriet imidlertid, at kravene til de private virksomheders pligt til at udpege databeskyttelsesrådgivere skal forstås meget snævert. Forbrugerrådet Tænk skal derfor opfordre til, at man fra dansk side vælger at udnytte hjemlen i forordningen til at vedtage nationale særregler om databeskyttelsesrådgivere jf. artikel 37, stk. 4. Vi foreslår i den forbindelse, at man sidestiller reglerne mellem private og offentlige virksomheders pligt til at udpege databeskyttelsesrådgivere.

§ 41, stk. 5 - Sanktioner

Forbrugerrådet Tænk noterer sig, at lovforslaget ikke indeholder en endelig stillingtagen til, hvorledes offentlige myndigheder skal sanktioneres. Forbrugerrådet Tænk finder det nødvendigt, at der også strammes op på myndighedernes håndtering af personlige oplysninger – ofte følsomme – hvilket, vi frygter ikke vil ske i samme grad som i den private sektor, hvis ikke myndigheder sanktioneres på lige fod. Henset til hvor gennemdigitaliseret et land Danmark er og de forholdsvis mange databrud som foregår i den offentlige sektor, skal vi opfordre til, at man indenfor rimelighedens grænser sidestiller offentlig og privat sektor i forhold til bødesanktioner. I den forbindelse gør vi opmærksom på, at det tilsyneladende er muligt i flertallet af de øvrige EU-lande, herunder Norge og Sverige.

Øvrige bemærkninger til lovforslaget

Forbrugerrådet Tænk skal opfordre til, at forordningens artikel 80 stk. 2, om repræsentation af forbrugerne, udnyttes nationalt, som forordningen åbner mulighed for. Ved at udnævne organisationer med adgang til at indgive klager til tilsynsmyndigheder og domstolene på vegne af forbrugere, også uden deres bemyndigelse, styrkes forbrugernes rettigheder væsentligt og lovgivningens præventive effekt øges betragteligt.

Nye digitale tjenester og produkter er kendetegnede ved deres kompleksitet og ved ofte at have mange brugere, hvilket netop gør gruppesøgsmål særligt relevant her. Desuden er Danmark et af de mest gennem digitaliserede lande i EU og danskerne nogle af de mest aktive, når det for eksempel kommer til brug af digitale medier. Derfor finder vi, at man fra dansk side, skal sikre denne mulighed i databeskyttelsesloven.

Forbrugerrådet Tænk uddyber gerne nærværende høringssvar, hvilket kan ske ved at kontakte seniorjurist Anette Høyrup på ah@fbr.dk eller tlf. 27 15 74 32.

Med venlig hilsen

Mette Raun Fjordside
Afdelingschef for politik og strategi

Anette Høyrup
Seniorjurist

Justitsministeriet
Att. Nanna Due Binø
Slotsholmsgade 10
1216 København K

Sendt pr. e-mail til databeskyttelseskontoret@jm.dk

14.08.2017

Forsikringsorganisationernes
Fællessekretariat F.M.B.A.
Philip Heymans Allé 1
2900 Hellerup
Tlf.: 41 91 91 91
Fax: 41 91 91 92
fp@forsikringogpension.dk
www.forsikringogpension.dk

Danske Bank 31004001060104
IBAN DK30 30004001060104
SWIFT-BIC DABADKKK

Claus Tønnesen
Juridisk rådgiver
Dir. 41919047
ct@forsikringogpension.dk

Sagsnr. GES-2017-00224
DokID 343301

Forsikring & Pensions bemærkninger til "Udkast til forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven)"

Forsikring & Pension har den 7. juli 2017 modtaget udkast til forslag til databeskyttelsesloven i høring med frist senest den 22. august 2017. Forsikring & Pensions bemærkninger til lovudkastet fremgår nedenfor. Eftersom formålet med lovudkastet først og fremmest er at supplere reglerne i databeskyttelsesforordningen, jf. de almindelige bemærkninger til lovforslaget, har Forsikring & Pension også bemærkninger af overordnet karakter til forordningen og Betænkning nr. 1565/2017.

Overordnede kommentarer til lovudkastet:

Indhentelse og behandling af person- og andre kundeoplysninger udgør centralnervesystemet i forsikringsselskabernes bedømmelse af risici og forsikringsbegivenheder. Dette er kerneområder i det at drive forsikrings- og pensionsvirksomhed. Det er derfor afgørende for de danske forsikrings- og pensionsselskaber, at reguleringen af selskabernes indhentning og anden behandling af personoplysninger er så enkel og klar som muligt.

Forsikring & Pension er på den baggrund bekymret over Justitsministeriets antagelse om, at der generelt efter databeskyttelsesforordningen er et vidt råderum for at opretholde og også indføre ny national regulering i forhold til behandlingen af artikel 6-oplysninger. Spørgsmålet om rammerne for supplerende national regulering er afgørende for forsikrings- og pensionsbranchen, der som bekendt helt tilbage fra 1998 ud over persondataloven også har været underlagt reglerne om videregivelse af kundeoplysninger i kapitel 9 i lov om finansiel virksomhed.

Det er derfor vigtigt for Forsikring & Pension at fremhæve, at forsikrings- og pensionsbranchen ikke er enig med ministeriet, når det i Betænkning 1565/2017, især pkt. 3.4.3.3, konkluderes, at bl.a. reglerne om videregivelse af kundeoplysninger i kapitel 9 i lov om finansiel virksomhed i deres helhed kan opretholdes. Forsikring & Pension er opmærksom på, at det flere steder i pkt. 3.4.3 i betænkningen fremhæves, at mulighederne for national regulering i forhold til private virksomheder er særlig klar i forhold til behandling efter artikel 6, stk. 1, litra c,

men dette billede sløres af, at det andre steder i teksten er uklart, om der alene refereres til behandling efter denne bestemmelse. Uklarheden forstærkes af den ikke ganske klare terminologi i brugen af bl.a. begreberne "præcisering af.." og "supplerende regulering".

Det er Forsikring & Pensions opfattelse, at er der inden for artikel 6's område kun er hjemmel til nationalt at stille supplerende krav til behandlingen af personoplysninger i forhold til behandlinger, der sker efter artikel 6, stk. 1, litra c og litra e.

Baggrunden for denne opfattelse er især selve formuleringen af artikel 6, hvor det i stk. 2 og 3 i artiklen præciseres, at der i forhold til behandlinger, som sker efter litra c og e, kan indføres "mere specifikke bestemmelser", og at grundlaget for behandlingen skal fremgå af EU-retten eller af medlemsstaternes nationale ret.

Efter Forsikring & Pensions opfattelse lægger den klare formulering af artikel 6, stk. 2 og 3 op til en modsætningsslutning, således at der ikke i forhold til behandlinger efter de øvrige litra i artikel 6, stk. 1, kan opstilles supplerende nationale krav, som skal være opfyldt, for at oplysningerne kan behandles. Dette stemmer også med forordningens generelle formål om at skabe ensartet retstilstand på området i hele EU.

Forsikring & Pension er opmærksom på, at formuleringen af visse præambelbetragtninger, herunder slutningen af præambelbetragtning 10, skaber en vis uklarhed, der dog ikke kan rokke ved den klare retstilstand, som er kommet til udtryk i formuleringen af artikel 6, stk. 2 og 3.

Forsikring & Pension skal anmode Justitsministeriet om at klargøre sin opfattelse på dette vigtige punkt. Er ministeriet ikke enig i Forsikring & Pensions ovennævnte opfattelse, anmoder Forsikring & Pension om, at spørgsmålet snarest muligt forelægges for Europa-Kommissionen.

Forsikring & Pension har følgende konkrete bemærkninger til lovudkastet:

1. Hjemmelen for behandling af følsomme oplysninger (lovudkastets § 7/Forordningens artikel 9, stk.2, litra f)

Det fremgår af lovudkastets § 7, stk. 1, at forbuddet i forordningens artikel 9, stk. 1 mod at behandle de i bestemmelsen opregnede personoplysninger, herunder helbredsoplysninger, bl.a. ikke gælder, når betingelserne i artikel 9, stk. 2, litra f er opfyldt, dvs. når "Behandling er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares, eller når…". Formuleringen af litra f svarer til bestemmelsen i Persondatalovens § 7, stk. 2, nr. 4.

Forsikring & Pension anser denne hjemmel og dens anvendelsesområde for helt central i forhold til selskabernes muligheder for på sikkert grundlag at behandle artikel 9-oplysninger på personforsikrings- og pensionsområdet. Det grundlæggende formål med en forsikrings- eller en pensionsaftale er således at muliggøre den registreredes fastlæggelse af et retskrav ved skadesanmeldelse og udbetaling af erstatning i hele aftaleperioden og også efter aftaleforholdets ophør, men dog indenfor eventuelle anmeldelses- og forældelsesfrister.

Den centrale betydning af bestemmelsen i § 7, stk. 1, jf. artikel 9, stk. 2, litra f, understreges af, at samtykke som behandlingshjemmel med databeskyttelsesforordningen er blevet mere usikker, hvilket ved flere lejligheder er påpeget af såvel Datatilsynet som Justitsministeriet. Der henvises i den forbindelse til bemærkningerne i Betænkning 1565/2017, s. 168-83, hvoraf fremgår, at forordningen som noget nyt, men samtidigt i upræcist omfang, skærper kravene til et samtykkes frivillighed og dermed skaber usikkerhed om samtykke som behandlingshjemmel. Denne usikkerhed vil efter Forsikring & Pensions opfattelse sandsynligvis også gøre sig gældende i forhold de former for samtykke, som kræves ved videregivelse ifølge lov om finansiel virksomhed og efter sundhedsloven ved udlevering af oplysninger fra sundhedsvæsenet. Dette forhold vil få meget væsentlig betydning for forsikrings- og pensionsselskaberne, da samtykke i en lang række situationer efter de to love er eneste vej til indhentning og kontrol af de nødvendige personoplysninger.

Forsikring & Pension skal på den nævnte baggrund foreslå, at det af bemærkningerne til § 7, stk. 1 kommer til at fremgå, at retskravshjemmelen i forhold til forsikrings- og pensionsområdet skal forstås således, at personoplysninger, der er eller kan vise sig at være relevante i forhold til opfyldelse af en forsikrings- eller en pensionsaftale, herunder bedømmelse af aktuelle og potentielle skadebegivenheder, kan behandles med hjemmel i bestemmelsen. Dette naturligvis forudsat, at selskaberne lever op til kravene i anden lovgivning, herunder sundhedslovens krav ved indhentelse af helbredsoplysninger fra sundhedssektoren.

Som yderligere begrundelse for det nævnte forslag henviser Forsikring & Pension til, at det helt grundlæggende i at drive forsikrings- og pensionsvirksomhed, som det er kommet til udtryk i forsikringsaftaleloven (§§ 21-23) og i erstatningsrettens almindelige principper om dokumentation for tab og tabsbegrænsningspligt, er, at forsikringsselskaberne har mulighed for at indhente og kontrollere de nødvendige oplysninger, for at selskaberne kan bedømme rejste erstatningskrav. Kan selskaberne ikke sikkert og på effektiv måde få disse oplysninger og kontrollere deres rigtighed, vil konsekvensen ofte være, at selskabet må nægte at betale erstatning eller evt. reducere erstatningen til skadelidte, hvilket næppe har været meningen med databeskyttelsesreglerne.

2. Forsikrings- og pensionsselskabers behandling af personoplysninger til statistiske formål (lovudkastets § 10/forordningens artikel 9, stk. 2, litra j)

§ 10, stk. 1 i lovudkastet indeholder en begrænsning i forhold til forordningens art. 89, stk. 1., som efter Forsikring & Pensions opfattelse ikke er hensigtsmæssig og næppe heller tilsigtet.

Det fremgår således af ordlyden i § 10, stk. 1, at oplysninger som nævnt i databeskyttelsesforordningens art. 9, stk. 1, og artikel 10 må behandles i følgende situationer (vores understregninger):

"… hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig af hensyn til udførelsen af undersøgelserne".

Art. 89, stk. 1 i forordningen indeholder ikke et krav om, at statiske formål eller undersøgelser skal have væsentlig samfundsmæssig betydning, idet bestemmelsen har følgende ordlyd:

"*Behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål skal være underlagt fornødne garantier for registreredes rettigheder og frihedsrettigheder i overensstemmelse med denne forordning".*

Desuden er formuleringen *"statistiske formål i overensstemmelse med artikel 89, stk. 1"* anvendt i de øvrige bestemmelser i forordningen, der omfatter behandling til brug for statistik, herunder i art. 9, stk. 2, litra j.

Det er afgørende for forsikrings- og pensionsselskaberne, at formuleringen i lovudkastets § 10, stk. 1, ikke er mere snæver end forordningens art. 89, stk. 1. Det skyldes, at selskaberne i vidt omfang og for at leve op til tilsynsmæssige krav i bl.a. Solvens II-reformen fra EU, der trådte i kraft 1. januar 2016, foretager behandling af personoplysninger til statistiske formål. Statistikkerne ligger til grund for aktuarmæssige beregninger af selskabernes forsikringsrisici og hensættelser til dækning af indtrådte skader mv. og danner i mange tilfælde grundlaget for selskabernes indberetninger til Finanstilsynet.

Økonomiske og administrative omkostninger ved lovforslaget

Forsikring & Pension har noteret sig, at lovudkastet ikke indeholder oplysninger om de økonomiske og administrative konsekvenser af forslaget for det offentlige og for erhvervslivet. Udkastet indeholder derimod nogle bemærkninger om øgede klagemuligheder for borgerne samt "visse negative administrative konsekvenser" for dem.

Forsikring & Pension er opmærksom på, at lovudkastet som altovervejende hovedregel er en videreførelse af gældende ret, samt at eventuelle yderligere økonomiske eller administrative byrder for det offentlige og for erhvervslivet ved databeskyttelsesreformen skyldes databeskyttelsesforordningen og dermed ikke dansk lovgivning.

Forsikring & Pension finder det imidlertid misvisende, at det ikke af lovudkastet klart fremgår, at lovudkastet er en del af en større EU-initieret reform, der utvivlsomt vil medføre meget betydelige både økonomiske og administrative omkostninger for det offentlige og for erhvervslivet såvel i implementeringsfasen som i driftsfasen. Det misvisende understreges af, at der med lovudkastet på væsentlige punkter lægges op til (videreførelse af) supplerende national regulering, og at det i øvrigt af Betænkning 1565/2017 klart fremgår, at forordningen efter Justitsministeriets opfattelse indeholder meget vide rammer for opretholdelse af eksisterende eller introduktion af ny, supplerende national regulering på området.

Afsluttende bemærkninger

Forsikring & Pension skal afslutningsvist beklage, at høringsperioden falder sammen med den generelle sommerferieperiode i Danmark, hvor det er overordentligt vanskeligt for Forsikring & Pension at drøfte det meget omfattende, og samtidigt for forsikrings- og pensionsselskaberne helt centrale høringsmateriale, med medlemmerne. Forsikring & Pension tillader sig på den baggrund at tage forbe-

hold for, at det senere i lovprocessen kan blive nødvendigt at fremkomme med yderligere bemærkninger, som det under andre forhold havde været muligt at medtage i nærværende høringssvar.

Forsikringsorganisationernes
Fællessekretariat F.M.B.A.

Sagsnr. GES-2017-00224
DokID 343301

Med venlig hilsen

Claus Tønnesen

DANSKE REVISORER FSR

Justitsministeriet
Slotsholmsgade 10
1216 København K
Att.: Fuldmægtig Nanna Due Binø

Pr. e-mail: databeskyttelseskontoret@jm.dk

22. august 2017

FSR – danske revisorer
Kronprinsessegade 8
DK - 1306 København K

Telefon +45 3393 9191
fsr@fsr.dk
www.fsr.dk

CVR. 55 09 72 16
Danske Bank
Reg. 4183
Konto nr. 2500102295

Udkast til forslag til databeskyttelsesloven – høringssvar

FSR – danske revisorer har haft lejlighed til at gennemgå lovudkastet til den nye databeskyttelseslov. Sammenholdt med den nye persondataforordning er der tale om et meget omfattende regelsæt, som stiller store krav til de enkelte virksomheder i forhold til efterlevelse og den fornødne dokumentation herfor.

Mange af reglerne er allerede at finde i persondataloven, og i den forstand er der ikke tale om nye regler, men realiteten er den, at langt de fleste virksomheder ikke har haft megen fokus på de gældende regler og reelt står for at skulle implementere det nye regelsæt helt fra bunden.

FSR – danske revisorer har i den forbindelse set på, hvordan revisorbranchen kan understøtte virksomhedernes arbejde med at sikre og demonstrere compliance – accountability og good governance - og hvordan dette dokumenteres på en transparent måde i forhold til kunder, samarbejdspartnere og myndigheder. Dette gennemgås i det følgende. Foreningen vil gerne benytte denne lejlighed til at orientere herom.

Herudover har foreningen en bekymring vedrørende fastsættelse af bødeniveauet, som fremgår afslutningsvist.

Lovpligtige krav om dokumentation for, at persondatareglerne overholdes

Med den nye persondataforordning understreges, at det ikke er nok blot at overholde reglerne. Man skal også kunne dokumentere, at man rent faktisk gør det.

FSR – danske revisorer har i den forbindelse udarbejdet en erklæring, som kan give virksomhederne en høj grad af sikkerhed for, at de efterlever reglerne, og som samtidig fungerer som lovpligtig skriftlig dokumentation[1].

[1] Link til udkast til FSR – danske revisorers erklæring på vores hjemmeside. Endelig udgave forventes offentliggjort primo september.

Mange virksomheder vil som en naturlig del af deres forretning have en rolle som databehandler og vil i så fald have en lovgivningsmæssig forpligtelse til at kunne dokumentere, at virksomheden overholder reglerne over for den dataansvarlige (typisk en kunde). Her vil en revisorerklæring være en enkel og sikker løsning.

Virksomheder, som outsourcer opgaver, der involverer persondata, har omvendt en forpligtelse til at kontrollere, at den virksomhed, som der outsources til, overholder en række bestemmelser i persondataloven.

Det er de færreste virksomheder, som har en kompetence in-house, som kan varetage en sådan opgave. Her vil den nye erklæring kunne anvendes på den måde, at den virksomhed, der outsources til, indhenter en erklæring om, at de overholder persondataloven.

Revisorerklæring i forbindelse med tilsyn med virksomhederne
Anvendelsen af revisorerklæringer giver også Datatilsynet en bedre mulighed for et risikobaseret tilsyn, da risikoen for manglende compliance er markant reduceret i en virksomhed, som har fået en erklæring, der med høj grad af sikkerhed fastslår, at reglerne er overholdt.

Dermed har Datatilsynet mulighed for at koncentrere sig om virksomheder, som ikke har en ekstern dokumentation for sin compliance. Dette har særligt betydning i en situation som den nuværende, hvor det ikke ser ud til, at Datatilsynet får tilført flere ressourcer til kontrol af, at de nye regler overholdes. Skal der dog reelt ske et løft i danske virksomheders overholdelse af reglerne og forståelse for formålet med databeskyttelsen, skal det gå hånd i hånd med et tilsyn, der har muligheden for at sikre efterlevelsen og får flere ressourcer.

Revisorerklæring som mærkningsordning
Forordningens artikel 43 og lovudkastet § 25 giver mulighed for at certificere databehandlere og dataansvarlige ved at indføre en slags mærkningsordning, hvor virksomheden kan skilte med, at de overholder persondataforordningen.

FSR – danske revisorer kan se mange fordele ved en sådan ordning, der kan være med til at skabe tillid mellem forbrugere og virksomheder. Netop tilliden til, at ens personoplysninger behandles forsvarligt, er afgørende, når mere og mere kommunikation, indberetning til myndigheder, køb af varer og ydelser m.v. foregår via internettet.

Foreningens nye erklæring kan anvendes som en mærkningsordning i den forbindelse, ved at virksomhederne skilter med, at de har indhentet en sådan erklæring. Der er allerede virksomheder, som oplyser på deres respektive hjemmesider, at de har en revisorerklæring som dokumentation for, at de overholder reglerne.

Administrative bøder
Endelig skal nævnes, at der lægges op til, at Datatilsynet kan udstede administrative bødeforlæg i sager, hvor virksomheden selv erkender, at der er sket en overtrædelse af reglerne.

Samtidig indføres der med forordningen nye og meget store bøderammer, men uden at der er en indikation af, hvor stor en bøde skal være for overtrædelse af de enkelte bestemmelser. Der vil dog formentlig blive tale om langt større bøder.

FSR – danske revisorer kan være lidt betænkelige ved, at det formentlig i en række tilfælde vil blive Datatilsynet, som fastsætter det nye niveau for bøder, uden at der er en domstol inde over. I sidste ende er det domstolene, som fastsætter straffen for overtrædelse af lovgivningen i Danmark, og ikke den udøvende myndighed.

Vetoret
Datatilsynet kan efter § 31 i særlige tilfælde forbyde overførsel af følsomme persondata til usikre tredjelande - hvilket er hjemlet ved forordningens art. 49.5. § 31 og lovbemærkningerne hertil angiver ikke nogen kriterier for, hvornår Datatilsynets "vetoret" kan anvendes. Da vetoretten kan være af afgørende betydning for virksomheder, som overfører data til visse tredjelande, bør det være mere klart, hvornår og hvorfor den kan bruges

I forhold til øvrige bemærkninger til udkastet, herunder mere detaljerede kommentarer til de enkelte bestemmelser, skal vi henvise til høringssvaret fra Dansk Erhverv, som vi i det hele tilslutter os.

Såfremt der er spørgsmål til ovennævnte, kan undertegnede kontaktes.

Med venlig hilsen

Brian Adrian Wessel
Faglig direktør

Ilinniartitaanermut, Kultureqarnermut, Ilisimatusarnermut Ilageeqarnermullu Naalakkersuisoqarfik
Departementet for Uddannelse, Kultur, Forskning og Kirke

NAALAKKERSUISUT
GOVERNMENT OF GREENLAND

Justitsministeriet
Databeskyttelseskontoret@jm.dk

22-08-2017
Sagsnr. 2017 - 15595
Dok. nr. 5973968

Postboks 1029
3900 Nuuk
Tlf: +299 34 50 00
Fax:+299 32 20 73
Email: ikiin@nanoq.gl
www.nanoq.gl

Høringssvar vedr forslag til databeskyttelseslov

Departementet har den 11. Juli 2017 fra Formandens Departement til videre foranstaltning fået oversendt høringsmateriale vedr. Forslag til databeskyttelseslov.

Departementet har i den forbindelse bedt om en udtalelse hertil fra Digitaliseringsstyrelsen, som er en styrelse under departementet.

På baggrund af styrelsens udtalelse skal departementet bemærke følgende.

Departementet udtrykker bekymring ved forslaget § 31. Da Grønland indtil videre stadig anses som et usikkert tredjeland, vil de samarbejder, som grønlandske myndigheder og virksomheder har med danske leverandører, være omfattet af denne bestemmelse.

For Grønland vil et forbud, en begrænsning eller suspendering af overførsel af personoplysninger ramme hårdt, både i den grønlandske myndighedsudøvelse og i det grønlandske erhvervsliv.

Grønlands Selvstyre forventer, at det kommende Datatilsyn vil administrere denne bestemmelse med lempelse i forhold til relationen mellem en grønlands dataansvarlig og en dansk databehandler. Det skal ses under hensyntagen til, at den grønlandske anordning om persondataloven indtil 30. november 2019 indeholder nogle overgangsordninger.

Måtte Datatilsynet finde fejl og mangler i relationen mellem en grønlandske dataansvarlig og en dansk databehandler, bør første påbud være, at parterne gives en rimelig tid til få bragt orden i forholdet, samt at Datatilsynet vejleder parterne i, hvordan forholdet kan bringes i overenstemmelse med det fremlagte forslag om databekyttelse.

Når der foreligger en vedtaget lov, vil Grønlands Selvstyre overveje muligheden for at udnytte forslagets § 48 om, at loven kan i kraftsættes ved kongelig anordning for Grønland med de ændringer, som de grønlandske forhold tilsiger.

Inussiarnersumik inuulluaqqusilluta
Med venlig hilsen

Claus Kleemann
Afdelingschef

HORESTA

Til
Justitsministeriet

Att. Databeskyttelseskontoret@jm.dk

Hotel • Restaurant
& Turisterhvervet

Vodroffsvej 32
1900 Frederiksberg C

Tel +45 35 34 80 80
Fax +45 35 24 80 88

www.horesta.dk
horesta@horesta.dk

cvr.nr. 17 01 46 11

21. august 2017
Journalnr.: 2017-0517/LMO

Vedr.: - Høringssvar vedr. udkast til Databeskyttelsesloven

HORESTA skal hermed afgive bemærkninger vedr. ovennævnte udkast til lovforslag.

For så vidt angår lovforslagets – herunder Persondataforordningens – betydning for hele arbejdsmarkedsområdet, skal HORESTA som medlem af Dansk Arbejdsgiverforening (DA), henvise til DA's høringssvar.

Databeskyttelsesloven skal supplere Persondataforordningens regler, som i vidt omfang vil finde direkte anvendelse i Danmark. De foreslåede regler i Databeskyttelsesloven tilsigter i vid udstrækning at sikre, at den særpraksis, man på visse områder har haft i DK, kan fortsættes. Et eksempel herpå er de undtagelser fra oplysningspligten, som fremgår af den foreslåede § 22. HORESTA hilser dette velkommen.

Det højere bødeniveau
Selvom persondataforordningens – og databeskyttelseslovens – regler i vidt omfang viderefører de eksisterende regler, så er der meget høj fokus på reglerne fra virksomhedernes side, hvilket naturligt hænger sammen med, at sanktionerne (bødeniveauet) skærpes kraftigt.

Mange virksomheder er naturligvis bekymrede for, om de vil få høje bøder for overtrædelser, som ikke er begået forsætligt, men alene på baggrund af simpel uagtsomhed og/eller uvidenhed. Der er således brug for, at Justitsministeriet udsender en vejledning, som mere konkret forklarer, hvilke typer af overtrædelser, der kan medføre bøder og forklarer, hvor bødeniveauet for de forskellige typer af overtrædelser kan forventes at komme til at ligge - herunder i gentagelsestilfælde.

HORESTA skal opfordre til, at bødeniveauet så vidt muligt holdes på lavest mulige niveau, særligt i begyndelsen af reglernes levetid, hvor mange virksomheder må forventes forsat at være i gang med en implementering af reglerne.

Det fremgår af den foreslåede § 41, stk. 5, at der endnu ikke er taget stilling til sanktionsspørgsmålet i forhold til offentlige myndigheder. Det er HORESTAs opfattelse, at der også bør fastsættes sanktioner i forhold til offentlige myndigheders overtrædelse af reglerne. Hvis ikke offentlige myndigheders overtrædelse sanktioneres vil incitamentet til at overholde reglerne, og sikre den fornødne sikkerhed, svækkes hos de offentlige myndigheder, og derudover vil det være krænkende for retsfølelsen for private virksomheder, som risikerer endog meget høje bøder.

Behov for mere konkret vejledning

HORESTA har, som en række andre organisationer, afholdt flere informationsmøder om den nye persondataforordning, og det er tydeligt at persondatareglerne – desværre – ikke alle steder har haft den fornødne bevågenhed. Der er meget tvivl om, hvad man skal og hvad man må – også i forhold til eksisterende regler. Her oveni kommer så nye regler i kraft af forordningen.

Justitsministeriet og Datatilsynet har planlagt udarbejdelse af en række meget detaljerede vejledninger omkring specifikke emner, som f.eks. om DBO-ordningen, samtykke, sikkerhed mv. Der er også planlagt en generel informationspjece om forordningen til udgivelse i september.

HORESTAs oplevelse er som sagt, at der er usikkerhed om reglerne, men også stor usikkerhed om, hvad man helt lavpraktisk skal gøre for, at komme på omgangshøjde både med eksisterende og nye regler.

Datatilsynet har udgivet "12 spørgsmål som dataansvarlige allerede nu med fordel kan forholde sig til". Denne pjece giver helt overordnet nogle anvisninger på, hvad virksomhederne skal være opmærksomme på, og hvad de skal gøre.

HORESTAS oplever imidlertid, at reglerne giver anledning til mange konkrete spørgsmål, og det er HORESTAs vurdering, at der er behov for en mere opfattende og operationel guide til, hvad man som virksomhed skal gøre (reglerne) og hvordan hele processen med at blive compliant både i forhold til eksisterende og nye regler mere praktisk kan gribes an.

Med venlig hilsen

Kaare Friis Petersen
Erhvervsjuridisk chef

Fra: Jeppe Rosenmejer [rosenmejer@hvr.dk]
Sendt: 21. august 2017 14:36
Til: £Databeskyttelseskontoret (951s26)
Emne: Forslag til databeskyttelseslov *NDB har en sag/LNJ

Håndværksrådet har ingen bemærkninger til det fremsendte lovforslag.

Med venlig hilsen
Jeppe Rosenmejer

Jeppe Rosenmejer
Chefkonsulent, cand.jur, LL.M.

tlf. +45 33 93 20 00
e-mail rosenmejer@hvr.dk

Ingeniørforeningen, IDA
Kalvebod Brygge 31-33
DK-1780 København V
Tlf. +45 33 18 48 48

Viden der styrker
ida.dk

databeskyttelseskontoret@jm.dk

Svar på Justitsministeriets høring over udkast til forslag til databeskyttelsesloven

22. august 2017

Hermed Ingeniørforeningen, IDAs høringssvar på Justitsministeriets høring over udkast til forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Indledende bemærkninger

IDA takker for muligheden for at kommentere på Justitsministeriets udkast til databeskyttelsesloven.

Indledende er det vigtigt for IDA at understrege, at Europaparlamentets og Rådets forordning nr. 2016/679 er et vigtigt fremskridt i forhold til at sikre en bæredygtig udnyttelse af de nye digitale muligheder med respekt for borgerne og individets rettigheder til at beskytte privatliv og bevare kontrollen med egne data, samt at styrke it-sikkerheden generelt.

Det er vigtigt, at vi sikrer de fordele, der er ved digitalisering både for erhvervsliv, forskning, borgerne og samfundsmæssigt. Der synes i materialet til høringen at være en tendens til at nedvurdere de muligheder, der ligger i forordningen og i stedet forsøge at opretholde status quo mest muligt. Forordningen er absolut et skridt i den rigtige retning. IDA skal derfor opfordre til, at man med databeskyttelsesloven bestræber sig på at udnytte de muligheder, der er i forordningen til at opgradere, modernisere og styrke både virksomheder og offentlige institutioner. Kun sådan kan vi bevare tilliden hos borgerne til at ville bruge de digitale muligheder, herunder f.eks. sociale medier og digital kommunikation med det offentlige. Dermed kan vi også styrke konkurrenceevnen hos danske virksomheder og sikre en effektiv offentlig sektor med opbakning blandt borgerne.

Til eksempel savner IDA i udkastet til databeskyttelsesloven en aktiv inddragelse af Privacy by Design og Privacy by Default, som den nytænkning det er, at gennemsigtighed, dataminimering og forbrugerkontrol tænkes ind i systemer fra starten af, jf. de syv grundprincipper, udarbejdet af Ann Cavoukian.

Et andet eksempel, hvor forslaget er for snævert i forhold til de muligheder, forordningen giver, er retten til at blive glemt. Ikke mindst i betragtning af, at Justitsministeriet foreslår at udnytte muligheden for at indhente tilsagn fra børn maksimalt ved at sætte grænsen helt ned til 13 år, er der behov for at sikre borgerne bedst muligt. Herunder også retten til at kunne få

berigtiget, blokeret eller slettet oplysninger, som viser sig at være uhensigtsmæssige og uønskede senere i livet. Det er derfor vigtigt, at den pligt som forordningen indeholder til at slette indsamlede oplysninger, hvis borgeren gør brug af sin ret til at tilbagekalde sit samtykke, trækkes frem i lovgivningen, så vel som i de efterfølgende vejledninger.

Endelig er brugen af kunstig intelligens og algoritmer til f.eks. at indsamle oplysninger om og lave beregninger til grundlag for f.eks. banklån, stærkt stigende. Det er derfor en væsentlig nyskabelse, at også algoritmer nævnes udtrykkeligt som en del af de automatiske behandlinger, man som forbruger skal give samtykke til. Dette kan med fordel trækkes frem i den danske databeskyttelseslov.

Bemærkninger til de enkelte afsnit

§3

Stk. 2: IDA finder, at denne undtagelse er alt for bred, da det her er hhv. politiets og forsvarets efterretningstjenester som institutioner, der fritages, og ikke konkrete aktiviteter. IDA vil opfordre til, at der sker en afgrænsende præcisering.

Stk. 3: På samme måde er formuleringen "oplysninger, der foretages som led i Folketingets parlamentariske arbejde" uklar og kan med fordel præciseres.

Stk. 10: Her savnes en præcis formulering af, hvorvidt undtagelsen kun gælder behandling af personoplysninger for ansatte i forsvaret, danske såvel som lokalt ansatte, eller om " i forbindelse med Forsvarets internationale operative virke" også omfatter andre borgeres personoplysninger, i udlandet eller herhjemme.

IDA er bekymret for, hvor vidtgående denne bestemmelse er. IDA vil opfordre til, at der sker en præcisering af, hvornår, der er grundlag for undtagelse og hvordan personkredsen, som kan være genstand for efterretninger, afgrænses. Der bør være en begrundet mistanke inden personoplysninger trækkes og anvendes i et efterretningsøjemed.

Behandling af personoplysninger

§5

Stk. 3: IDA finder det bekymrende, at der i §5, stk. 3 gives en minister mulighed for at tillade, at personoplysninger må viderebehandles til andre formål, end de oprindeligt var indsamlet til. Set sammen med forslagets §23, hvor oplysningspligten ikke finder anvendelse, når myndigheder viderebehandler personoplysningerne til et andet formål end det, hvortil de er indsamlet, synes det at være i grundlæggende strid med det overordnede formål med forordningen at give borgerne større kontrol over egne data.

IDA er grundlæggende imod denne bestemmelse og er bekymret for, at denne bestemmelse kan udvande tilliden til, at de oplysninger man overlader i det offentliges varetægt, kun bruges til det formål de er afgivet. Dermed kan bestemmelsen medføre modvilje og skepsis i forhold til at benytte den offentlige sektors digitale services. IDA skal dermed opfordre til, at bestemmelsen i §, stk. 3 fjernes.

§6

Stk. 2: IDA anerkender, at børn også har stor fordel af at kunne benytte digitale tjenester, herunder f.eks. gaming og sociale medier. Når man, som i dette lovforslag, udnytter muligheden for at nedsætte alderen til kun 13 år, kræver det imidlertid, at man strammer så meget desto mere op på beskyttelsen af borgernes private oplysninger, retten til at blive glemt, tilsynet med at reglerne overholdes og at der udvikles specifikke vejledninger om, hvordan man indhenter tilsagn fra børn.

IDA skal derfor opfordre til, at man i resten af databeskyttelsesloven tager i betragtning, at reglerne også skal kunne beskytte børn, at tilsynet med reglerne styrkes, og at der udarbejdes vejledning rettet mod de helt unge forbrugere, både til børnene og til de virksomheder, der har produkter målrettet denne yngste aldersgruppe.

§7 og §8

Der ligger omkring disse to paragraffer en udfordring i, at oplysninger, som tidligere efter dansk praksis har været klassificeret som personoplysninger, nu falder uden for regelsættet. Det betyder bl.a., at private dataansvarlige i nogle tilfælde ikke længere skal indhente forudgående tilladelse fra Datatilsynet. IDA mener, at disse forhold, herunder f.eks. oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold, bør re-klassificeres. Det kan være som almindelige eller følsomme oplysninger, men det bør ikke stå tilbage, at disse oplysninger nu automatisk bliver opfattet som almindelige oplysninger under forordningen.

IDA opfordrer derfor Justitsministeriet til at gennemgå og foreslå re-klassicificering af de personoplysninger, der tidligere har været en del af dansk praksis, men som nu falder udenfor.

§11

Stk. 2 og 3: IDA er bekymret for, at Justitsministeriet med lovforslaget understøtter private virksomheders brug af cpr-numre som en del af den almindelige drift. Mange borgere opfatter deres cpr-nummer som en privat og sikker oplysning. I praksis er det også cpr-nummeret, der bruges som identifikation overfor f.eks. sundhedsmyndighederne, eller når børn skal skrives op til skole og lignende. Denne sammenblanding af identifikationsmiddel til meget private anliggender og f.eks. mere eller mindre tilfældige køb af varer eller tjenester på nettet, er med til at øge risikoen for identitetstyveri og datamisbrug. Hvis virksomheder skal kunne - direkte eller indirekte – kræve at få kendskab til borgerens cpr-numre for f.eks. at ville sælge en tjeneste, bør der udvikles en anden og mere sikker måde at identificere sig over for det offentlige.

IDA opfordrer til, at reglerne om private virksomheders brug præciseres og begrænses, indtil der evt. er fundet et mere egnet og sikkert identifikationsmiddel til brug for borgerens kontakt med offentlige systemer.

§13
IDA kan støtte en videreførelse af de nuværende regler, som siger, at en virksomhed ikke må videregive oplysninger om en forbruger til en anden virksomhed, medmindre forbrugeren har givet sit udtrykkelige samtykke. Ligesom de generelle kundeoplysninger uden krav om samtykke ikke må omhandle følsomme oplysninger eller oplysninger om børn under 13 år, medmindre forældrene har givet samtykke.

Der er imidlertid brug for at en præcisering af reglerne i forhold til de virksomheder, også kaldet "databrockere", som har som forretningsområde at indsamle og videresælge digitale oplysninger, indsamlet på internettet, via mobiltelefonen eller via apps. Borgernes data har i sig selv en enorm værdi ved videresalg, og man bør derfor heller ikke her kunne omgå reglerne om udtrykkeligt samtykke. Af lovforslagets nuværende ordlyd er det uklart, hvorvidt disse nye markedsføringsmetoder, hvor data deles mellem virksomheder digitalt, er omfattet.

IDA skal opfordre til, at databeskyttelsesloven udfattes på en måde, så der ikke hersker tvivl om borgernes rettigheder; heller ikke på de nye forretningsområder, som eksempelvis handel med data.

Uafhængige tilsynsmyndigheder

Datatilsynet
En forordning og/eller en lov er ikke bedre end den dertilhørende håndhævelse. IDA identificerer med hhv. forordningen samt nærværende lovforslag, at adskillige opgaver pålægges Datatilsynet. Alene forordningen oplister 22 forskellige opgaver i artikel 57 og dertil kommer tilsyneladende tillægsopgaver i nærværende lovforslag. Er ekstra opgaver i sig selv et problem? Nej, det er de ikke. Men de bliver det, når der ikke følger ressourcer med. I nærværende lovforslag fremgår der ikke noget om tilførsel af ekstra ressourcer til Datatilsynet til brug for håndhævelsen af persondataforordningen, samt dette lovforslag. Endvidere har man under overskriften "3. Økonomiske og administrative konsekvenser for det offentlige" på side 249 i lovforslagets "Almindelige bemærkninger" valgt ikke at skrive yderligere ligesom det sammenfattende skema på side 251-252 står tomt. Dette finder IDA stærkt bekymrende! Der venter Datatilsynet en kæmpe opgave og på nuværende tidspunkt tilføres de ifølge lovforslaget ikke flere ressourcer. Det er afgørende, at der afsættes både midler og tid til at opruste, således at Datatilsynet den 25. maj 2018 er helt klar til opgaven.

Vi har på nuværende tidspunkt både en kommende omfattende persondataforordning samt en digitalisering, som "buldrer" derudaf, herunder øget omfang af data og øget anvendelse af data. Ingen af delene er nogen nyhed – ej heller noget, som man skal tage letsindigt på. Ikke desto mindre kan IDA konkludere, at Datatilsynet ikke just er fulgt med denne udvikling, idet antallet af årsværk i Datatilsynet er faldet siden 2011 og har de sidste 4-5 ligget stabilt (lavt), jf. nedenstående tabel:

Tabel 1. Antallet af årsværk i Datatilsynet (2011-2017)

År	Årsværk	Indeks 2011 = 100
2017	33,4	92
2016	32,3	88
2015	33,4	92
2014	33,7	92
2013	33,8	93
2012	31,6	87
2011	36,5	100

Kilde: Moderniseringsstyrelsens forhandlingsdatabase.
Note: 2011 er indeks 100.

IDA appellerer på det kraftigste med dette høringssvar, at Datatilsynet styrkes markant

Retsmidler, ansvar og sanktioner

§ 41
Stk. 5: IDA noterer sig, at der fortsat udestår en afklaring af, hvordan og hvorledes offentlige myndigheder skal sanktioneres, såfremt de overtræder hhv. persondataforordningen samt nærværende lovforslag. Allerede i dag har de ikke-eksisterende sanktionsmuligheder konsekvenser for Datatilsynet i forhold til de offentlige myndigheder, jf. Version2's artikel den 9. august 2017 "Datatilsynet: Vi bliver sat skakmat, når myndigheder ignorerer vores kritik". IDA finder det problematisk, at der endnu ikke er taget stilling hertil, og kan kun opfordre til, at et udspil herom sendes i høring snarest.

IDA finder det i lighed med bl.a. *Forbrugerrådet Tænk* og *Rådet for Digital Sikkerhed* nødvendigt, at der også strammes op på myndighedernes håndtering af personlige oplysninger – ofte følsomme. Hvis ikke myndighederne sanktioneres på lige fod med den private sektor, frygter vi, at alvoren ikke indtræffer i tilstrækkeligt omfang i de offentlige myndigheder – herunder i samme grad som i den private sektor. Når vi derudover tager i betragtning, hvor gennemdigitaliseret et land Danmark er, samt de forholdsvist mange databrud, som foregår i den offentlige sektor, skal vi i IDA opfordre til, at man inden for rimelighedens grænser sidestiller offentlig og privat sektor i forhold til bødesanktioner. IDA erklærer sig i den sammenhæng enig med Rådet for Digital Sikkerhed i forhold til følgende oplistning af bøder som sanktionsmiddel:

1. For det første har det en betydeligt større afskrækkende effekt, at der kan trækkes penge ud af et budget til bøder, end at der kan komme et brev fra Datatilsynet, hvori der udtales kritik. Bøder er med andre ord et meget stærkt incitament til at overholde loven.
2. For det andet et det vigtigt for retfærdighedsopfattelsen i samfundet, at der er lighed for loven. Den samme overtrædelse skal straffes ens uanset, om man er offentlig eller privat.
3. For det tredje er det vigtigt, at der sker harmonisering i Europa. Danmark bør ikke være et discount land, når det kommer til at straffe overtrædelser i den offentlige

sektor. Når borgerne desuden skal være mobile jf. det indre marked, vil det forekomme besynderligt, hvis de lande, de agerer i, straffer de offentlige myndigheder forskelligt.

Endelig gør vi opmærksom på, at det tilsyneladende er muligt at nå til enighed om sanktionering af offentlige myndigheder i flertallet af de øvrige EU-lande, herunder Norge og Sverige.

Ingeniørforeningen, IDA er overordnet meget positive over for forordningen og dermed også for en dansk implementering. Vi anser en god og klar lovgivning med respekt for individets rettigheder for afgørende for, at vi kan fortsætte med at udnytte de mange fordele og muligheder, der er i digitalisering.

Med venlig hilsen

Grit Munk
Chefkonsulent
Politik, Analyse og Presse

Helena Juul Jensen
Chefkonsulent
Politik, Analyse og Presse

INSTITUT FOR
MENNESKE
RETTIGHEDER

Justitsministeriet
Slotsholmsgade 10
1216 København K
Danmark
databeskyttelse@jm.dk

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
DIREKTE

ANPE@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 17/01251-3

22. AUGUST 2017

HØRING OM FORSLAG TIL LOV OM SUPPLERENDE BESTEMMELSER TIL FORORDNING OM BESKYTTELSE AF FYSISKE PERSONER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER OG OM FRI UDVEKSLING AF SÅDANNE OPLYSNINGER (DATABESKYTTELSESLOVEN)

Justitsministeriet har ved e-mail af 10. juli 2017 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til udkast til forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Indledningsvis ønsker instituttet at takke Justitsministeriet for det store og grundige arbejde, der ligger bag såvel Betænkning nr. 1565 (herefter "betænkningen") som udkast til ny databeskyttelseslov.

Instituttet har sammen med Forbrugerrådet Tænk og Rådet for Digital Sikkerhed deltaget i det for betænkningen forudgående arbejde med at gennemgå Databeskyttelsesforordningen (herefter "forordningen") i forhold til gældende dansk ret. Instituttet finder det positivt, at en række af de forslag og bemærkninger, som Forbrugerrådet Tænk og instituttet afgav i denne forudgående proces, er blevet indarbejdet i betænkningen. Instituttet takker Justitsministeriet for muligheden for at deltage i processen, og vil benytte nærværende høring til at tilkendegive nogle centrale bemærkninger og bekymringer over for Justitsministeriet.

Instituttet har følgende bemærkninger:

GENERELT

Databeskyttelsesforordningen har til hensigt at sikre en stærkere og mere effektiv beskyttelse af personoplysninger på tværs af medlemsstaterne.

Forordningen fastslår, at retten til databeskyttelse er en grundlæggende rettighed efter EU's Charter om grundlæggende rettigheder og Traktaten om Den Europæiske Unions funktionsmåde (TEUF). Forordningens præambel understreger, at globaliseringen og den teknologiske udvikling har skabt nye udfordringer for beskyttelse af personoplysninger. Denne udvikling kræver stærkere og mere sammenhængende databeskyttelsesregler i EU såvel som en effektiv håndhævelse af disse regler.

Selvom den endelige forordning ikke er helt så nyskabende, som det oprindeligt var hensigten, er det forordningens eksplicitte hensigt at skærpe beskyttelsesniveauet og håndhævelsen af reglerne på en række områder. Det er i dette lys, at forordningen skal fortolkes og implementeres i dansk ret. Som instituttet bemærker i sin årlige Statusrapport, har Datatilsynet og Rigsrevisionen gentagne gange påpeget, at efterlevelsen af persondataloven er mangelfuld, ikke mindst i de offentlige institutioner.

På trods af at der er både økonomiske og administrative omkostninger forbundet med implementeringen, bør man derfor se forordningen som en kærkommen lejlighed til at foretage en grunding gennemgang af persondataretten og styrke databeskyttelsesniveauet, hvor dette er muligt. Som understreget i forordningens præambel er en effektiv databeskyttelsesramme helt afgørende både for udviklingen af en stærk digital økonomi og for borgernes tillid til at benytte digitale services.

Det er imidlertid ikke det indtryk, man får, når man læser betænkningen. Justitsministeriet finder på en lang række områder, at forordningens bestemmelser er overensstemmende med dansk lov og retspraksis, og at derfor kun skal ske mindre ændringer i forhold til gældende ret.

Justitsministeriet nedtoner således forordningens nyskabelser, og i lovforslagets afsnit 1.2 bliver det konkluderet, at forslaget i vidt omfang er en videreførelse af gældende ret.

Instituttet er enigt i, at der på flere områder er tale om en videreførelse af gældende dansk ret. Men her er det vigtigt at er, at formålet med forordningen er at styrke databeskyttelsesniveauet såvel den praktiske efterlevelse af reglerne.

- Instituttet anbefaler, at forordningen fortolkes og implementeres i lyset af, at hensigten med forordningen er at sikre en stærkere og mere effektiv databeskyttelse på tværs af medlemsstaterne.

På områder hvor der er tale om nyskabelser eller skærpede krav er det vigtigt, at disse ikke nedtones i en sådan grad, at myndigheder og

virksomheder får indtrykket af, at det er godt nok at fortsætte som hidtil, og først på tidspunktet for en eventuel sikkerheds- eller databeskyttelsesbrist bliver bevidste om, at dette alligevel ikke var tilstrækkeligt.

Tilsvarende gælder i relation til en nyskabelse som privacy by design i forordningens artikel 25. Det fremgår af betænkningens afsnit 5.2.3 (side 418), at bestemmelsen ikke medfører et krav om at re-designe samtlige ældre systemer, såfremt der kan etableres et passende sikkerhedsniveau for disse systemer på anden vis, herunder ved undervisning, interne procedurer og tilsvarende organisatoriske foranstaltninger. Som Justitsministeriet bemærker på side 423, skal samtlige systemer dog leve op til alle forordningens øvrige krav fra "dag 1", hvorfor der er flere gode grunde til at sikre, at systemerne allerede kan leve op til alle forordningens krav fra dennes ikrafttrædelse.

Der er også tale om en nyskabelse i forordningens artikel 35, som vedrører brugen af konsekvensanalyser. Ifølge Artikel 29-gruppen udgør konsekvensanalyser et vigtigt redskab for den dataansvarlige til at sikre, at reglerne overholdes, samt til dokumentation herfor. Det fremgår imidlertid af betænkningens afsnit 5.13.3 (side 525), at den dataansvarlige i de fleste tilfælde ikke vil være forpligtet til at foretage en konsekvensanalyse, og at bestemmelsen derfor vil få et forholdsvis begrænset anvendelsesområde.

Instituttet er bekymret for, at man hermed nedtoner det ansvar, forordningen reelt pålægger den dataansvarlige, herunder de skærpede krav til dokumentation, som konsekvensanalyser kan være med til at løfte, uanset om den dataansvarlige er direkte forpligtet til at foretage analysen i den konkrete situation.

En systematisk gennemførelse af konsekvensanalyser vil ikke kun styrke databeskyttelsesniveauet til gavn for den registrerede, men kan også støtte den dataansvarliges daglige arbejde med at overholde reglerne og undgå brud på datasikkerheden.

- Instituttet anbefaler, at forordningens nyskabelser ikke nedtones i en sådan grad, at eksisterende problemer blot udskydes til det tidspunkt, hvor der opstår en databeskyttelses- eller sikkerhedsbrist.
- Instituttet anbefaler, at man i højere grad understreger fordelene ved at foretage systematiske konsekvensanalyser og anbefaler konsekvent brug heraf.

Selv hvor der ikke umiddelbart synes at være tale om nyskabelser, er det afgørende, at man tager i betragtning, at den virkelighed, de nye regler skal implementeres og anvendes i, på mange måder er en helt anden, end den hvori persondatadirektivet og persondataloven blev

vedtaget. Det betyder, at regler, som er videreført i deres helhed eller udelukkende med små justeringer, kan have en væsentlig anden betydning og praktisk anvendelighed i dag. Dette gælder blandt andet reglerne om ret til at gøre indsigelse mod automatiske individuelle afgørelser efter forordningens artikel 22.

Det er derfor helt afgørende, at databeskyttelsesloven såvel som forordningen ledsages af nogle tidssvarende eksempler, der eksemplificerer og illustrerer over for både dataansvarlige og databehandlere samt de registrerede, i hvilke situationer reglerne rent faktisk kan komme i spil. Dette er ikke i tilstrækkeligt omfang tilfældet i hverken betænkning eller lovforslag.

- Instituttet anbefaler, at betænkningen, lovbemærkninger samt kommende vejledninger ledsages af tidssvarende eksempler, der tager højde for den digitale virkelighed, der møder myndigheder, borgere og virksomheder.

Udover materielle nyskabelser har forordningen også til hensigt at skabe en stærkere og mere effektiv beskyttelse af personoplysninger gennem en øget grad af harmonisering. På trods af at forordningen giver vid mulighed for nationale undtagelser og særregler, er det vigtigt, at adgangen hertil benyttes varsomt, så danske særregler ikke kommer til at forhindre en ensartet beskyttelse på tværs af medlemsstaterne. Adgangen til at fastsætte nationale særregler bør derfor begrænses til situationer, hvor disse er med til at styrke individets rettigheder, og gerne med inspiration fra Artikel 29-gruppen.

- Instituttet anbefaler, at Danmark kun benytter adgangen til at fastsætte nationale særregler, hvor dette bidrager til en styrkelse af individets rettigheder, og gerne med inspiration fra Artikel 29-gruppen.

Instituttet finder i øvrigt anledning til at bemærke, at den måde, hvorpå forordningen implementeres i dansk ret, gør det vanskeligt at få et overblik over forpligtelser og rettigheder efter forordningen. Dette gælder ikke mindst for almindelige borgere, der skal forstå deres retsstilling. Selvom der er tale om en forordning, der således gælder direkte i medlemsstaterne, bliver denne implementeret i dansk ret ved databeskyttelsesloven. Loven ledsages dels af betænkningen på mange hundrede sider, dels af lovforslagets bemærkninger, der også udgør flere hundrede sider. Hertil kommer, at loven ikke kan stå alene, men i vidt omfang henviser til forordningen. Instituttet er opmærksomt på, at det med ønsket om nationale særregler er nødvendigt at operere både med forordningsteksten og danske regler, men i praksis betyder det, at det er nødvendigt at orientere sig i flere forskellige og meget omfangsrige retskilder, når man skal have et overblik over retstilstanden.

- Instituttet anbefaler, at der sideløbende med vedledningerne til loven udarbejdes offentligt tilgængeligt materiale, der på letforståelig vis beskriver borgerens rettigheder efter forordningen.

Endelig må det forventes, at Datatilsynets arbejdsbyrde vil blive øget markant, når forordningen træder i kraft.

Dette gælder navnlig forpligtelsen til at fremme kendskabet til og forståelsen af forordningen efter artikel 57, stk. 1, litra a, b, og d, der som Justitsministeriet bemærker i betænkningens afsnit 7.5.3, må antages at komme meget mere i fokus bl.a. som følge af det fremadrettede sanktionsniveau, samarbejdet med andre tilsynsmyndigheder efter artikel 57, stk. 1, litra g og h, der bliver udbygget og formaliseret, samt forpligtelsen efter artikel 57, stk. 1, litra i, til at holde øje med relevant udvikling. Henset til sanktionsniveauet må det imidlertid også antages, at de øvrige opgaver, herunder dem, der allerede gælder i dag, kommer til at kræve flere ressourcer, navnlig i de kommende år, hvor fortolkningen af forordningen skal fastlægges.

En af de generelle nyskabelser er overgangen fra anmeldelsespligt til en risikobaseret tilgang. Det betyder, at den dataansvarlige som hovedregel ikke længere skal anmelde databehandlinger til Datatilsynet, men må foretage en risikobaseret vurdering af egne databehandlinger. For at de dataansvarlige kan foretage en sådan vurdering, er det afgørende, at Datatilsynet har tilstrækkelige juridiske, tekniske og formidlingsmæssige ressourcer til at bistå dem, der har behov herfor. Dette er en afgørende forudsætning for gennemførelsen af forordningen.

- Instituttet anbefaler, at Datatilsynet styrkes, således at tilsynet har tilstrækkelige juridiske, tekniske og formidlingsmæssige ressourcer til at løfte sine opgaver efter forordningen.

Som det nævnes flere steder, sker der en markant ændring af sanktionsniveauet. Instituttet støtter forslaget i lovforslagets § 42 om, at Datatilsynet bemyndiges til at udstede administrative bødeforlæg i ukomplicerede sager uden bevismæssige tvivlsspørgsmål.

Allerede på nuværende tidspunkt har muligheden for at lade offentlige myndigheder ifalde bødeansvar givet anledning til debat. I lovforslaget er der imidlertid ikke taget stilling til spørgsmålet.

Det skærpede sanktionsniveau bliver nævnt som en af forordningens vigtigste nyskabelser, og varslet om et ændret bødeniveau har fået forventningerne om en bedre og mere effektiv beskyttelse til at stige. Dette skaber allerede nu incitamenter til at forbedre databeskyttelsen hos dataansvarlige og databehandlere landet over.

Instituttet understreger vigtigheden i, at alle borgere sikres det samme beskyttelsesniveau uanset hvem, der behandler deres personoplysninger. En effektiv håndhævelse af forordningen over for samtlige dataansvarlige og databehandlere, uanset om der er tale om private virksomheder eller offentlige myndigheder, er derfor helt central for forordningens gennemførelse.

I forlængelse af disse generelle bemærkninger følger her uddybende bemærkninger til en række af forordningens og lovens bestemmelser.

GENERELLE BEHANDLINGSPRINCIPPER – FORORDNINGENS ARTIKEL 5-11 OG DATABESKYTTELSESLOVENS §§ 5-14

Indledningsvis bemærkes, at den dataansvarliges ansvar for overholdelsen af de generelle behandlingsprincipper skærpes. Efter direktivets artikel 6, stk. 2, påhviler det den dataansvarlige at "sikre", at principperne blev overholdt, mens den dataansvarlige efter forordningens artikel 5, stk. 2, skal kunne påvise overholdelsen.

Forordningen understreger med andre ord vigtigheden af de generelle principper. Det er derfor vigtigt, at de forbedringer, præciseringer mv., der er blevet tilføjet disse principper, ikke bliver nedtonet i en grad, der underminerer denne overordnede skærpelse.

Forordningens artikel 5(1)(a) – gennemsigtighed

I betænkningens afsnit 3.1.3 (side 92) fremhæver Justitsministeriet, at det af Kommissionens oprindelige forslag til forordning fremgår, at princippet om "gennemsigtighed" er en nyskabelse. Princippet tilsigter, at al behandling af personoplysninger bør være lovlig, rimelig og gennemsigtig. Det vil sige, at enhver information eller kommunikation til den registrerede, herunder i forbindelse med den oplysningspligten og indsigtsretten i forordningens kapitel 3, bør være lettilgængelig og letforståelig.

Der er her tale om en nyskabelse, som udover at være et generelt behandlingsprincip også kan få betydning for fortolkningen af bestemmelserne i forordningens kapitel 3. Instituttet finder det derfor beklageligt, at Justitsministeriet på side 93 konkluderer, at der ikke er tale om en ændring i forhold til gældende ret.

Selvom det fortsat vil være tilsynsmyndigheden, der fastlægger det nærmere indhold af princippet om god databehandlingsskik, vil tilsynsmyndigheden nu være nødsaget til specifikt at inddrage princippet om "gennemsigtighed".

- Instituttet anbefaler, at det fremhæves, at der med princippet om gennemsigtighed i forordningens artikel 5(1)(a) er tale om en nyskabelse, og at Datatilsynet inddrager princippet i sin fastlæggelse af princippet om god databehandlingsskik.

Forordningens artikel 5(1)(b) og 6(4) og lovens § 5 – Formålsbestemthed og samkøring

Der er i forslaget lagt op til en svækkelse af princippet om formålsbestemthed. Dette gælder navnlig i forhold til lovforslagets § 5, stk. 3, hvor der lægges op til, at der inden for rammerne af forordningens artikel 23 kan fastsættes nærmere regler om, at offentlige myndigheder må behandle personoplysninger til andre formål, end dem de oprindeligt blev indsamlet til, uafhængigt af, om disse formål måtte være uforenelige med de oprindelige formål.

Selvom forordningens artikel 23 giver adgang til at undtage bl.a. fra kravet om formålsbestemthed, er det afgørende, at denne adgang benyttes undtagelsesvist, da en fravigelse af dette for persondataretten helt centrale princip kan føre til en generel svækkelse af borgernes databeskyttelse.

- Instituttet anbefaler, at adgangen til at undtage fra kravet om formålsbestemthed i lovens § 5, stk. 3, jf. forordningens artikel 23, kun anvendes undtagelsesvist og efter en konkret vurdering, og at man uddyber hvorfor, det er nødvendigt at foretage netop denne undtagelse.

En tilsvarende problemstilling gælder i relation til reglerne om samkøring. Uafhængigt af EU-retten stilles der efter gældende dansk ret krav om, at der for samkøring i kontroløjemed skal være særskilt lovhjemmel. Dette har styrket borgernes rettigheder i en tid, hvor offentlige myndigheder indsamler og behandler stadigt flere oplysninger om borgerne og ønsker at dele disse oplysninger med andre myndigheder. Det fremgår af betænkningens 3.1.3.2 (side 97), at Justitsministeriet har vurderet, at det efter forordningen fortsat vil være muligt – i forarbejderne til databeskyttelsesloven – at operere med en sådan forudsætning.

Instituttet finder det derfor beklageligt, at man ikke viderefører denne retstilstand. Dette skyldes, at Justitsministeriet vurderer, at navnlig forordningens artikel 5 og artikel 6(4) yder en tilstrækkelig beskyttelse af den registreredes rettigheder og samtidigt efterkommeroffentlige myndigheders behov for samkøring. Instituttet er ikke enigt i denne vurdering. Instituttet anerkender, at der kan være et konkret behov for at samkøre oplysninger, men finder, at man som minimum bør have Folketinget godkendelse, og den gennemsigtighed, der følger med behandlingen af et forslag om særskilt lovhjemmel. En øget mulighed for samkøring uden særskilt lovhjemmel set sammen med ovenstående mulighed for at undtage fra kravet om formålsbestemthed medfører en substantiel svækkelse af borgernes rettigheder.

- Instituttet anbefaler, at man fastholder kravet om særskilt lovhjemmel til samkøring.

Forordningens artikel 5(1)(c) – Dataminimering

Justitsministeriet fremhæver i betænkningens afsnit 3.1.3 (side 92), at der i Kommissionens oprindelige forslag til forordning blev lagt op til en præcisering af princippet om dataminimering. Det fremgår i den forbindelse af præambelbetragtning nr. 39, at personoplysninger kun må behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde. Her er der således tale om en skærpelse af princippet om dataminimering.

Det fremgår imidlertid af betænkningens side 97, at ordlyden er stort set enslydende med persondatalovens § 5, stk. 3, hvorfor der ikke kan være tiltænkt en anden indholdsmæssig betydning.

Selvom præambelbetragtning nr. 39 alene udgør et fortolkningsbidrag, finder instituttet Justitsministeriets konklusion misvisende. Det bør fremhæves i lovforslagets bemærkninger, at forordningen præciserer princippet, og at dansk ret må tilpasses i nødvendigt omfang.

- Instituttet anbefaler, at lovforslagets bemærkninger præciseres, så det fremgår, at der er tale om en skærpelse af princippet om dataminimering.

DEN REGISTREREDES RETTIGHEDER

Ligesom det er afgørende for at sikre individets ret til privatliv og databeskyttelse, at de generelle behandlingsprincipper som beskrevet ovenfor bliver fortolket i lyset af forordningens formål om at styrke databeskyttelsesniveauet, er det vigtigt, at den registreredes rettigheder bliver fortolket og fastlagt i dette lys. Forordningen lægger generelt op til en styrkelse af den registreredes rettigheder, og det er vigtigt, at dette ikke nedtones i den danske implementering.

Det er bl.a. også i relation til den dataansvarliges oplysningspligt og den registreredes ret til indsigt, berigtigelse og sletning, at betydningen af den digitale virkelighed, som reglerne skal fortolkes og anvendes i, spiller ind. Dette betyder, at selv mindre justeringer og præciseringer kan få stor betydning i praksis, og det er afgørende, at de kommende vejledninger til databeskyttelsesloven indeholder konkrete tidssvarende eksempler, der illustrerer bestemmelsers reelle indhold gennem.

De oplysninger, som den registrerede har brug for, således at denne kan udøve sine rettigheder efter forordningen, ændrer sig i takt med den teknologiske udvikling. Der sker f.eks. i stadigt større omfang automatisk behandling af personoplysninger gennem algoritmer. Det betyder, at den registrerede i dag, til forskel fra tidligere har et stadigt større behov for viden om disse algoritmer, herunder til en vis grad relevant teknisk viden. For at den almindelige borger kan bruge oplysningerne, stilles der dermed også stadigt større krav til gennemsigtighed efter forordningens artikel 12.

Instituttet er enigt i, at der også efter direktivet gælder et princip om gennemsigtighed, og at princippet derfor ikke som sådan er nyt, men den digitale virkelighed har ændret sig, og det er vigtigt, at man fortolker og anvender både princippet om gennemsigtighed, men også det efterfølgende krav til underretningspligt og indsigtsret i lyset heraf.

Der er derfor centralt, at denne nyskabelse ikke nedtones, men i stedet illustreres med tidssvarende eksempler i betænkningen, lovforslaget og de efterfølgende vejledninger.

Eksempelvis er der i relation til oplysningspligten i forordningens artikel 13(1)(c) tale om en nyskabelse, idet der nu også skal henvises til retsgrundlaget for behandlingen. I betænkningens afsnit 4.3.3 (side 287) foreslår Justitsministeriet, at dette krav blot kan tilføjes i et "ansøgningsskema eller lignende". Dette giver udmærket mening i en ikke-digital kontekst, men store dele af den databehandling, der sker i dag, finder sted online. Princippet kan muligvis overføres til den online kontekst, men teksten bør ledsages af tidssvarende eksempler, så der ikke opstår tvivl herom.

- Instituttet anbefaler, at kapitlet om den registreredes rettigheder i betænkningen, lovforslaget og vejledninger bliver ledsaget af tidssvarende eksempler, der illustrerer både egentlige nyskabelser, og giver konkrete eksempler fra borgerens digitale virkelighed.

Forordningens artikel 22 – Ret til indsigelse og automatiske individuelle afgørelser

Brugen af automatiske afgørelser på baggrund af algoritmer får stadigt større og større betydning. Selvom der i noget omfang er tale om en videreførelse af gældende ret, er den virkelighed, forordningen skal fortolkes i, som anført ovenfor en helt anden end den, direktivet er blevet fortolket i. Forordningens artikel 22 må derfor forventes at få en langt større betydning end sin forgænger.

Instituttet savner helt overordnet en definition / præcisering af begrebet "automatisk individuel afgørelse", herunder hvilke situationer, der reelt er tale om. I den forbindelse savner instituttet også flere digitale eksempler f.eks. fra sociale medier mv., da flere af de anførte eksempler beskriver situationer, hvor afgørelsen lige så godt kunne være blevet truffet manuelt.

- Instituttet anbefaler, at der, evt. i en vejledning, suppleres med flere tidssvarende eksempler, der illustrerer i hvilke situationer, den registrerede kan gøre indsigelse mod automatiske individuelle afgørelser.

Der henvises til Justitsministeriets sagsnummer: 2016-7910-0021.

Med venlig hilsen

Rikke Frank Jørgensen
SENIOR FORSKER

Anja Møller Pedersen
PHD STIPENDIAT

Justitsministeriet
Databeskyttelseskontoret
Att.: Jakob Lundsager
Slotsholmsgade 10
1216 København K

Sendt pr. mail: databeskyttelseskontoret@jm.dk

22. august 2017

Høring over udkast til forslag til databeskyttelsesloven

ISOBRO er medlem af Dansk Erhverv, og vi kan helt og fuldt tilslutte os deres høringssvar vedr. databeskyttelsesloven med følgende bemærkninger:

ISOBRO er brancheforening for indsamlingsorganisationer. Vi repræsenterer ca. 400 store og små foreninger, som målt på omsætning udgør ca. 90 % af indsamlingsmarkedet.

Vi har to forhold, som vi særligt vil fremhæve:

1.
Vi er særligt bekymrede for de store bødeforlæg for den store gruppe af mindre foreninger. Det forekommer ikke rimeligt, at en lille forening med sparsomme administrative ressourcer og begrænsede (personfølsomme) data skal kunne mødes af et bødekrav, mens det offentlige muligvis kan fritages. Vi vil derfor foreslå, at alle § 8 A godkendte organisationer undtages for bødekravet.

2.
Vi har naturligvis noteret os, at anvendelsesområdet ikke gælder for behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter. Artikel 2 stk. 1 C.

Stort set alle § 8 A godkendte organisationer har frivillige tilknyttet, der er engageret i organisationens arbejde på forskellig vis. Det er forholdsvist lige til, at konkludere at den frivillige kommunikationsdame, der kommer 3 timer om ugen, skal betragtes som ansat f.s.v.a. persondataforordningen.

Men i regi af foreningen foregår ofte en lang række frivillige aktiviteter, hvor der spontant foregår udveksling af data, som ledelsen i sagens natur ikke altid er vidende om.

Som eksempel kan nævnes en gruppe frivillige i en frikirke, som har organiseret en strikkeklub for menighedens unge mødre, hvor de kan komme og er velkomne til at invitere deres veninder med, og dér lære at reparere tøj eller strikke huer, vanter mv. Der føres naturligvis en liste over deltagerne, så man kan SMS'e til hinanden. Den gemmes formentlig på en privat pc eller mobiltelefon, men hvis én melder sig ud, har administrationen i menigheden ikke mulighed for at vide, at vedkommende melder sig ud denne liste eksisterer.

For mange frikirker er hjemmegrupper helt centrale for menighedslivet. Det er ofte et forum, hvor man kan invitere nye medlemmer med, eller personer som ikke er kirkevante, og gerne vil mødes med andre kristne i et mere intimt forum end til en gudstjeneste. Der bliver naturligvis udvekslet mail og mobilnumre. Men hvis en melder sig ud, har administrationen i menigheden ikke en jordisk mulighed for at vide, at denne liste eksisterer.

Problemstillingen i disse to eksempler gælder mange små foreninger. Det gør det svært, for ikke at sige umuligt, at efterleve kravene til den registreredes rettigheder, da det bryder med den lille forenings eller kirkes måde at fungere på, systematisk at skulle registrere hvem, der kommer hos hvem og har inviteret hvilke venner med.

ISOBRO vil derfor foreslå, at der udarbejdes en særlig vejledning til brug for foreningslivet, og vi stiller os naturligvis gerne til rådighed i den forbindelse.

ISOBRO

Robert Hinnerskov
Generalsekretær

Indsamlingsorganisationernes Brancheorganisation
Peter Bangs Vej 1, 5. – 2000 Frederiksberg
Tlf. 38 38 46 80 - Fax. 38 38 46 89 - E-mail isobro@isobro.dk

IT-Branchens svar på høring om ny databeskyttelseslov

IT-Branchen hilser Persondataforordningen velkommen og glæder sig over, at de nye regler skal sikre borgernes rettigheder i forbindelse med behandling af persondata og sikre prioritering af datasikkerhed i både virksomheder og offentlige institutioner.

IT-Branchen finder det afgørende, at den danske implementering af forordningen understøtter dansk erhvervs konkurrencevilkår både nationalt og på tværs af EU's medlemslande. Der er brug for et både moderne, fleksibelt og specifikt regelsæt, der ikke er for omkostningsfuldt for erhvervslivet at efterleve.

I den sammenhæng er IT-Branchen glade for, at lovforslaget indeholder flere gode tiltag til forsimpling og modernisering af de eksisterende regler, fx ved at fjerne sikkerhedsbekendtgørelsen, kategorien semi-følsomme data og krigsreglen.

Vejledning udestår
På trods af det nye lovforslag samt Justitsministeriets omfangsrige betænkning om dansk implementering af persondataforordningen er der fortsat mange udeståender og mange forhold, hvor afklaring afhænger af de kommende vejledninger.

Virksomhederne har særligt et stort behov for konkret afklaring om, hvordan mange af de nye krav i forordningen skal fortolkes og håndteres. Blandt andet dataportabilitet, retten til at blive glemt og niveauet for tilpas sikkerhed i forskellige behandlingssituationer - herunder behovet for logning.

IT-Branchen opfordrer Justitsministeriet til hurtigst muligt at sikre afklaring af disse udeståender og involvere branchen tæt i udformning af vejledningerne.

Også processen og ansvaret for vurdering og løbende opdatering af listen over sikre tredjelande er fortsat uklar. Lovgivning, sikkerhedssituation etc. er levende størrelser, og det er afgørende for global forretningsførelse, at man kender til listen og processen omkring den.

Husk folkeoplysning
Persondataforordningen indeholder flere nye krav til virksomhederne, men også en række vigtige nye rettigheder, ikke mindst til borgerne.

Hvis vi skal sikre en god dansk implementering af persondataforordningen, er det ikke blot vigtigt med vejledning og rådgivning rettet mod virksomheder, men også mod borgere. Et øget kendskab i befolkningen til rettigheder og klagemuligheder vil være med til at sikre en god anvendelse af de nye muligheder og en bedre forventningsafstemning omkring, hvornår og hvordan de nye regler kan anvendes.

IT-Branchen foreslår, at regeringen i forbindelse med den kommende finanslov afsætter midler specifikt til dette formål.

Offentlige sanktioner
IT-Branchen finder det beklageligt, at der endnu ikke er taget stilling til offentlige sanktioner.

IT-Branchen anbefaler, at der ligesom for private skal være klare sanktioner for det offentlige forbundet med manglende overholdelse af forordningen

Der er et stort behov for at opprioritere datasikkerheden i det offentlige. Fx slog Rigsrevisionen november 2016 fast, at alt for mange offentlige myndigheder sjusker med datasikkerhed.

Borgerne er lige glade med, om et databrud skyldes en fejl i offentlige myndigheder eller private virksomheder, og ofte vil der være mere følsomme data i de offentlige myndigheder med større konsekvenser for de berørte personer.

Samtidig vil det også medføre en konkurrencemæssig udfordring, hvis det offentlige ikke pålægges sanktioner, særligt på områder hvor det offentlige og private opererer på samme marked. Det er konkurrenceforvridende, når en privat virksomhed i sit tilbud skal indregne risikoen for at måtte blive idømt en bøde for overtrædelse af persondatareglerne, mens dette ikke er tilfældet for den offentlige virksomhed.

Der er afgørende for at opnå den nødvendige prioritering af databeskyttelse i det offentlige, at brud på reglerne har en alvorlig konsekvens. Styrket datasikkerhed kræver, at den enkelte offentlige myndighed eller institution prioriterer de nødvendige ressourcer. Det sker ikke uden stærke incitamenter.

Endvidere vil sanktioner til offentlige myndigheder sikre en synlighed omkring manglende datasikkerhed hos den øverste ledelse.

IT-Branchen anerkender, at det vil være uheldigt, hvis fx et hospital skal fyre flere læger og sygeplejersker som konsekvens af en bøde, og foreslår derfor en model for offentlige sanktioner, som samlet set holder de offentlige myndigheder udgiftsneutrale, men som sikrer, at der foretages den nødvendige prioritering af datasikkerheden.

Dette kan fx sikres ved at bøderne betales til en særlig pulje, der øremærkes at løse den pågældende myndigheds udfordringer med databeskyttelse. Det vil give en de facto omprioritering af midler til it-sikkerhed/databeskyttelse, og bødestørrelsen kan fastsættes efter de omkostninger det skønnes, at myndigheden skal bruge på at forhindre lignende databrud i fremtiden.

Substansbemærkninger

Ud over ovenstående generelle bemærkninger, har IT-Branchen følgende konkrete bemærkninger til lovforslaget:

§3, stk. 9
Geografisk begrænsning erstatter krigsreglen
Justitsministeriet lægger i lovforslaget op til at indføre en ny version af den såkaldte krigsregel. Justitsministeren bemyndiges til efter forhandling med vedkommende minister, at *fastsætte regler om, at personoplysninger, der behandles i nærmere bestemte IT-systemer, og som føres af eller for den offentlige forvaltning alene må opbevares her i landet.*

Det er positivt, at Justitsministeriet benytter anledningen til at gentænke den såkaldte krigsregel, og det er positivt, at det nu skal være undtagelsen og op til særlig afgørelse, hvis databehandlingsmulighederne skal begrænses. Det er endvidere positivt, at der understreges, at reglerne alene fokuserer på hensyn til statens sikkerhed.

IT-Branchen mener dog, helt generelt, at krigsregelen bør afskaffes, og ikke erstattes af ny ordlyd.

IT-Branchen er uenige i, at kravet om at databehandling skal ske på dansk grund, i sig selv er med til at sikre en øget databeskyttelse. Der findes i dag flere tekniske sikkerhedsforanstaltninger der kan sikre, at følsomme data beskyttes, også uden data behøver at være placeret i Danmark.

Der findes flere uklarheder i den nye formulering, der gør det usikkert, hvorvidt der reelt er tale om en indskrænkelse eller udvidelse af den gamle krigsregel. Det er fx uklart, i hvilket omfang

Justitsministeriet og ressortministerierne i praksis vil benytte sig af muligheden for at begrænse databehandlingsmulighederne, samt hvad man i praksis vil kategorisere under begrebet "statens sikkerhed".

§5
Garantier
I §5 stk. 5 omtales "kryptering" og "pseudonymisering" som *garantier*.
IT-Branchen vurderer, at der er tale om en uheldig oversættelse af den oprindelige forordningstekst, hvor begrebet "safeguards" er brugt.

Kryptering og pseudonymisering vil aldrig være en garanti, men kan være meget effektive sikkerhedsforanstaltninger. IT-Branchen foreslår at ordlyden ændres herefter.

§6
Aldersgrænser for samtykke
Justitsministeriet foreslår, at aldersgrænsen for behandling af personoplysninger om børn uden krav om forældresamtykke sættes til 13 år, hvilket er lavest muligt.

IT-Branchen støtter denne lave grænse, da det vurderes at sikre bedst mulig digital inklusion og dannelse. Der er rigtig mange danske unge under 16 der benytter sociale medier. Regler om samtykke bør ikke være en stopklods for at de unge kaster sig ud i at anvende ny teknologi.

§11
Semi-følsomme data
IT-Branchen finder det positivt, at Justitsministeriet lægger op til at fjerne datatypen "semi-følsom". Dette er en væsentlig forudsætning for, at CPR-nummeret fortsat kan behandles af både offentlige og private organisationer.

§13
Markedsføring
Den nuværende danske persondatalov indeholder særlige regler for anvendelse og videregivelse af personoplysninger til markedsføringsmæssige formål i persondatalovens § 6, stk. 2-4, § 12 og § 36, som i lovforslaget erstattes af § 13.

Det er IT-Branchens holdning, at generelle kundeoplysninger som for eksempel teledata og OIS-data frit skal kunne videregives uden samtykke til markedsføringsmæssige formål. Den registrerede har flere muligheder for at frasige sig modtagelsen af markedsføringsmateriale, blandt andet muligheden for udeladt nummer samt Robinsonlisten. Disse bør fortsat sikre den registreredes ret til at frabede sig uanmodede henvendelser med henblik på markedsføring.

IT-Branchen bemærker dog, at det fortsat er uafklaret om navne- og nummeroplysninger, de såkaldte 118-teledata i § 31 i lov om elektroniske kommunikationsnet og -tjenester (teleloven), er omfattet af de særlige regler i persondatalovens § 6, stk. 2-4, § 12 og § 36.

Datatilsynet har i en tidligere afgørelse j.nr. 2004-215-0160, om videregivelse af telefonbogsoplysninger tilkendegivet, at videregivelse af rene nummeroplysningsdata omfattet af § 34 i lov om konkurrence og forbrugerforhold på telemarkedet, som erstattes af § 31 i teleloven, *ikke* er omfattet af de særlige markedsføringsregler i persondatalovens § 6, stk. 2-4 og § 36. Videregivelse af teledata er derfor ifølge hovedreglen i § 6 stk. 1 underlagt kravet om samtykke. Afgørelsen er efter vores opfattelse forkert.

IT-Branchen mener, at teledata, som er ikke-følsomme oplysninger, såsom bl.a. navn og telefonnummer, bør udgøre en generel kundeoplysning. For at komme den uklarhed til livs,

opfordrer vi til, at forkaste kravet om samtykke, men at spørgsmålet om videregivelse af personoplysninger til markedsføringsmæssige formål alene vurderes efter interesseafvejningsreglen i persondataforordningens artikel 6 stk. 1, litra f).

IT-Branchen efterspørger derfor en vejledning med nærmere angivne retningslinjer for interesseafvejningsreglen og hvorledes en sådan vurdering skal foretages efter persondataforordningens artikel 6, stk. 1, litra f).

Vi stiller gerne op

IT-Branchen ser frem til den fortsatte dialog om dansk implementering af Persondataforordningen, og vi står naturligvis til rådighed for en uddybning af ovenstående.

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendt per email til
databeskyttelseskontoret@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 : 22. august 2017

Høringssvar vedr. udkast til forslag til databeskyttelsesloven

IT-Politisk Forening har følgende bemærkninger til Justitsministeriets forslag til databeskyttelsesloven (supplerende bestemmelser til databeskyttelses-forordningen 2016/679/EU).

Vores høringssvar henviser flere steder til den vedtagne tyske lov med supplerende bestemmelser til databeskyttelsesforordningen, "Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680" (fremover: "den tyske GDPR-lov"). Vi har i den forbindelse brugt den engelske oversættelses af loven, som det tyske indenrigsministerium har udgivet 14. juli 2017 [1].

Strukturen i høringssvaret følger lovforslagets paragraffer, med undtagelse af det sidste afsnit i høringssvaret, som vedrører muligheden for at tilsynsmyndighederne skal kunne anlægge en sag ved domstolen, hvis tilsynsmyndigheden mener at en tilstrækkelighedsvurdering fra EU-Kommissionen bør annulleres (jf. præmis 65 i Schrems-dommen C-362/14).

Undtagelser for efterretningstjenesterne (§ 3, stk. 2)

Lovforslagets § 3, stk. 2 har en generel undtagelse for behandling af personoplysninger, som udføres for Politiets Efterretningstjeneste (PET) og Forsvarets Efterretningstjeneste (FE). Det begrundes med at

databeskyttelsesforordningen jf. artikel 2, stk. 2, litra a) ikke gælder under udøvelse af aktiviteter, der falder uden for EU-retten, herunder statens sikkerhed.

IT-Politisk Forening vil anbefale, at undtagelsen i lovforslagets § 3, stk. 2 formuleres som en undtagelse vedrørende udøvelsen af aktiviteter der falder uden for EU-retten hos PET og FE, i stedet for en generel undtagelse vedrørende institutionerne PET og FE som sådan.

FE har eksempelvis opgaver vedrørende cybersikkerhed, som næppe fuldt ud kan dækkes af undtagelsen vedrørende statens sikkerhed. I den forbindelse skal det bemærkes, at EU-direktivet 2016/1148/EU om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for informationssystemer i hele Unionen ("NIS-direktivet") skal gennemføres inden 9. maj 2018, og at NIS-direktivet i artikel 2, stk. 1 forudsætter, at personoplysninger behandles i overensstemmelse med direktiv 95/46/EF (databeskyttelsesdirektivet). Hvis Center for Cybersikkerhed skal indgå i den danske gennemførelse af NIS-direktivet, kan en fuldstændig undtagelse fra databeskyttelsesforordningen næppe opretholdes.

Viderebehandling til andre formål (§ 5, stk. 3)

Efter § 5, stk. 3 kan vedkommende minister fastsætte regler i bekendtgørelsesform om, at personoplysninger af offentlige myndigheder må viderebehandles til andre formål, herunder videregives til andre dataansvarlige. Der er ikke noget krav om at det nye formål skal være foreneligt med det oprindelige, og der er således tale om en begrænsning af borgernes rettigheder, som skal opfylde betingelserne i databeskyttelsesforordningens artikel 23, jf. artikel 6, stk. 4.

Bestemmelsen skaber ikke i sig selv en hjemmel til at viderebehandle personoplysninger til andre formål, idet der først skal udarbejdes en bekendtgørelse inden for rammerne af artikel 23. Det er ikke ud fra lovforslagets bemærkninger muligt at vurdere hvilke typer viderebehandling og videregivelse, som beføjelsen vil blive brugt til, herunder i hvilket omfang § 5, stk. 3 også vil blive brugt til at fastsætte regler om viderebehandling og videregivelse for særlige kategorier af personoplysninger

(følsomme personoplysninger), jf. forordningens artikel 9.

IT-Politisk Forening finder det meget betænkeligt at give ministre så vidtgående beføjelser. Viderebehandling af personoplysninger til andre formål og ikke mindst videregivelse til andre myndigheder (dataansvarlige) har vidtgående konsekvenser for borgernes ret til privatliv og databeskyttelse. I mange tilfælde vil der være tale om særdeles følsomme personoplysninger. Sådanne beslutninger bør tages af Folketinget, som kan udstikke passende rammer i en lov, hvorefter den relevante minister eventuelt i bekendtgørelsesform kan fastsætte mere præcise regler, hvis Folketinget finder at det er hensigtsmæssigt.

Efter databeskyttelsesforordningens betragtning 41 kræver et retsgrundlag eller en lovgivningsmæssig foranstaltning ikke nødvendigvis en lov, som er vedtaget af et parlament. Det afgørende er at der foreligger et retsgrundlag eller en lovgivende foranstaltning, som er klar og præcis samt forudsigelig for de berørte personer, jf. retspraksis fra Den Europæiske Menneskerettighedsdomstol (EMD) og EU-Domstolen.

I den forbindelse vil IT-Politisk Forening dog anføre, at hensigten med betragtning 41 næppe er at alle beslutninger om udarbejdelse af et retsgrundlag eller en lovgivningsmæssig foranstaltning skal delegeres fra parlamentet til en minister. Det vil i øvrigt også være i strid med den danske parlamentariske tradition, at Folketinget uden andre begrænsninger end dem, som følger af EU-retten, overdrager den lovgivningsmæssige kompetence til regeringen på et så væsentligt område som behandlingen af borgernes personoplysninger i den offentlige sektor.

Udover spørgsmålet om kompetencefordelingen mellem regeringen og Folketinget, er IT-Politisk Forening stærkt bekymret for vurderingen af, om de lovgivningsmæssige foranstaltninger i bekendtgørelsesform overholder de konkrete betingelser i databeskyttelsesforordningens artikel 23. Bekendtgørelser har modsat love ingen bemærkninger, som nærmere kan uddybe hvordan en bestemmelse skal fortolkes, og der er ikke en udvalgsbehandling i Folketinget, hvor medlemmer af Folketinget kan stille spørgsmål til ministeren for at afklare, hvordan en bestemmelse skal fortolkes. Der er selvsagt

heller ikke mulighed for at fremsætte ændringsforslag.

Selvom udkast til bekendtgørelser sendes i offentlig høring, ligesom det er tilfældet med udkast til lovforslag, er der typisk ikke samme offentlige opmærksomhed omkring bekendtgørelser. Der er også et meget stort antal bekendtgørelser, som hvert år sendes i høring, og det kan blive en nærmest uoverkommelig opgave for eksempelvis civilsamfundsorganisationer som IT-Politisk Forening at monitorere, analysere og vurdere nye bekendtgørelser, som kan indebære viderebehandling af personoplysninger til andre formål. Den opgave vil være meget mere overkommelig, hvis bekendtgørelser er fast forankret i konkrete love, som udstikker retningslinjerne for hvad der kan fastsættes i bekendtgørelsesform.

Med den foreslåede § 5, stk. 3 ser IT-Politisk Forening en overhængende risiko for, at personoplysninger, som borgere har afgivet til én offentlig myndighed til bestemte formål, vil blive genanvendt til en lang række andre formål uden at borgerne er klar over det. Den fuldstændige begrænsning af oplysningspligten ved viderebehandling i henhold til § 5, stk. 3, som Justitsministeriet foreslår i databeskyttelseslovens § 23, gør risikoen for at borgernes personoplysninger i hemmelighed vil flyde rundt i det offentlige system, uden at borgerne er klar over det, endnu større.

Behandling af personoplysninger om strafbare forhold (§ 8)

I forhold til persondatalovens § 8 omfatter databeskyttelseslovens § 8 alene strafbare forhold, og altså ikke tillige væsentlige sociale problemer og andre rent private forhold. Det kan godt give anledning til visse betænkeligheder, at legitim interesse nu i princippet kan være et almindeligt behandlingsgrundlag for personoplysninger om væsentlige sociale problemer og andre rent private forhold (selvfølgelig med de begrænsninger som følger af anden lovgivning, eksempelvis straffelovens kapitel 27). Men databeskyttelsesforordningens artikel 10 omfatter kun strafbare forhold, og der er ikke på samme måde som i databeskyttelsesdirektivet mulighed for at udvide definitionen af særlige kategorier af personoplysninger.

I forhold til behandling af personoplysninger om strafbare forhold er den foreslåede § 8 stort set en videreførelse af de nuværende regler i persondataloven. I bemærkningerne til § 8, stk. 3 anføres det, at privates behandling af personoplysninger om strafbare forhold uden samtykke kun kan ske under meget snævre rammer, som for eksempel registrering af oplysninger om strafbare forhold med henblik på politianmeldelse.

Men § 8, stk. 3 vil også skulle dække dataansvarlige, som ved systematisk overvågning af internettet indsamler oplysninger om dynamiske IP-adresser med henblik på at retsforfølge påståede krænkelser af ophavsretslige rettigheder (”ulovlig fildeling” via eksempelvis ”Popcorn Time”), og eventuelt videregivelse af sådanne oplysninger til politiet. Denne systematiske behandling af en stor mængde oplysninger om strafbare forhold rejser nogle yderligere problemstillinger i forhold til behandling af personoplysninger for at anmelde konkrete lovovertrædelser, som en virksomhed (dataansvarlig) har konstateret, eksempelvis oplysninger fra TV-overvågning i forbindelse med et indbrud eller butikstyveri, eller digitale spor fra log-filer el.lign. i en sag om IT-kriminalitet.

Efter IT-Politisk Forenings opfattelse er der i sådanne situationer med systematisk dataindsamling behov for yderligere retsgarantier for den registrerede. Det skyldes ikke mindst, at det nuværende krav om anmeldelse og forudgående tilladelse hos tilsynsmyndigheden for behandling af oplysninger om strafbare forhold, jf. persondatalovens § 50, stk. 1, nr. 1), bortfalder når databeskyttelsesforordningen finder anvendelse fra 25. maj 2018. Et krav om forudgående godkendelse giver tilsynsmyndigheden mulighed for at fastsætte vilkår for behandlingen, for eksempel hvor længe personoplysninger må opbevares, hvis en beslutning om retsforfølgelse udsættes. Den dataansvarlige kan måske have et ønske om at vurdere omfanget af den påståede ophavsretslige krænkelse inden der eventuelt tages skridt til retsforfølgning eller politianmeldelse.

En mulighed for at fastsætte passende garantier for den registreres rettigheder kunne være at stille krav om høring og indhentning af forudgående tilladelse hos tilsynsmyndigheden inden en sådan systematisk

behandling af personoplysninger om strafbare forhold igangsættes, og at tilsynsmyndigheden får mulighed for at fastsætte vilkår for behandlingen ligesom det er tilfældet i dag. Det vil i praksis antageligt kun berøre ganske få dataansvarlige (der bedriver privat efterforskning), men have stor betydning for mange registreredes rettigheder. Databeskyttelsesforordningens artikel 36, stk. 5 må kunne udgøre en hjemmel for at fastsætte et sådant krav i databeskyttelsesloven.

Begrænsning af oplysningspligt og ret til indsigt (§ 22, stk. 1)

Lovforslagets § 22, stk. fastsætter en undtagelse fra oplysningspligten (artikel 13 og 14) og retten til indsigt (artikel 15), hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv. Det svarer til formuleringen i persondatalovens § 30, stk. 1.

Der er tale om en begrænsning af oplysningspligten og retten til indsigt udover de undtagelser som allerede følger af databeskyttelsesforordningen (artikel 13, stk. 4, artikel 14, stk. 5 og artikel 15, stk. 4). Idet hjemlen til § 22, stk. 1 må være databeskyttelsesforordningens artikel 23, vil IT-Politisk Forening anbefale, at der i bemærkningerne er en mere specifik henvisning til de(n) relevante del(e) af artikel 23. Artikel 23, stk. 2 kræver lovgivningsmæssige foranstaltninger med specifikke bestemmelser.

IT-Politisk Forening finder det problematisk, at § 22, stk. 1 med formuleringen ”den registreredes interesse i oplysningerne” kan lægge op til en interesseafvejning mellem den dataansvarliges og den registreredes interesser for alle anmodninger om indsigt. Det samme gælder i forhold til den dataansvarliges opfyldelse af oplysningspligten, især efter artikel 14.

En eventuel afvisning af indsigt må for alle anmodninger skulle begrundes i en konkret hjemmel i enten databeskyttelsesforordningens artikel 15, stk. 4 eller specifikke begrænsninger fastsat i databeskyttelsesloven ud fra forordningens artikel 23, stk. 1. Hvis der ikke er en specifik grund, for eksempel forretningshemmeligheder

eller håndhævelse af civilretlige krav (”andres rettigheder”, jf. forordningens betragtning 63), skal den registrerede havde indsigt i oplysningerne, uanset om den dataansvarlige ud fra en subjektiv vurdering måtte mene, at den registreredes interesse i oplysningerne er beskeden.

IT-Politisk Forening finder det positivt, at der med ”afgørende hensyn til private interesser” i § 22, stk. 1 og bemærkningerne hertil, lægges op til en begrænset anvendelse af denne undtagelse fra oplysningspligten og indsigtsretten. I forhold til kravet i databeskyttelses-forordningens artikel 23, stk. 2 om specifikke bestemmelser, kan det dog stadig betvivles, om ”afgørende hensyn til private interesser” er tilstrækkeligt klart og præcist.

Generel begrænsning af oplysningspligt og ret til indsigt (§ 22, stk. 2)

Lovforslagets § 22, stk. 2 svarer i sin struktur til persondatalovens § 30, stk. 2. Der er tale om en generel bestemmelse, som giver mulighed for at begrænse rettighederne efter databeskyttelsesforordningens artikel 12-15 (generelle betingelser om gennemsigtighed, oplysningspligt og indsigtsret), hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige interesser, hvor alle punkter (litraer) i artikel 23, stk. 1 medtages.

Efter IT-Politisk Forenings opfattelse er det tvivlsomt, om en sådan meget generel bestemmelse er forenelig med databeskyttelsesforordningens artikel 23. Selvom artikel 23, stk. 1 i forordningen har store ligheder med databeskyttelsesdirektivets artikel 13, stk. 1, udgør forordningens artikel 23, stk. 2 en afgørende forskel mellem forordningen og direktivet. Efter artikel 23, stk. 2 skal medlemsstaterne vedtage lovgivningsmæssige foranstaltninger med specifikke bestemmelser for at begrænse den registreredes rettigheder. Derudover stiller betragtning 41 krav om klarhed og præcision, og at anvendelsen af lovgrundlaget (her begrænsningen) skal være forudsigelig for de berørte personer, jf. retspraksis fra EMD og EU-Domstolen.

§ 22, stk. 2 er formuleret som en generel (”catch all”)

undtagelsesbestemmelse baseret på ”afgørende hensyn til offentlige interesser”, som supplerer undtagelsen i § 22, stk. 1. Forordningens artikel 23, stk. 2 lægger op til, at de specifikke bestemmelser bl.a. omfatter en specifikation af de dataansvarlige som begrænsningen gælder for, men det er ikke klart, om det ud fra ”offentlige interesser” kan konkluderes, at § 22, stk. 2 alene kan anvendes af dataansvarlige i den offentlige sektor. En eventuel afgrænsning af § 22, stk. 2 til dataansvarlige i den offentlige sektor vil dog næppe i sig selv være tilstrækkeligt til, at kravene om specifikke bestemmelser i forordningens artikel 23, stk. 2 kan siges at være opfyldt.

IT-Politisk Forening er opmærksom på, at bemærkningerne til lovforslagets § 22, stk. 2 (side 298-299) indeholder henvisninger til punkterne i forordningens artikel 23, stk. 2, men efter vores vurdering er der overladt alt for store skøn til den dataansvarlige. Det er problematisk i forhold til kravet om en forudsigelig anvendelse. De specifikke bestemmelser efter artikel 23, der begrænser indsigtsretten eller oplysningspligten, bør også fastsætte passende garantier for at beskytte den registrerede interesser. Den opgave kan ikke fuldstændigt overlades til den dataansvarlige.

Den tyske GDPR-lov indeholder i §§ 32-34 begrænsninger af oplysningspligten og indsigtsretten, som er noget mere specifikke end § 22, stk. 1-2 i det danske lovforslag. I den tyske GDPR-lov skelnes der bl.a. mellem private og offentlige dataansvarlige, og der er ikke en fuldstændig oplistning af alle begrundelser fra artikel i 23, stk. 1 (alle litraer) i de specifikke bestemmelser, som begrænser henholdsvis oplysningspligten og indsigtsretten.

Begrundelser for at begrænse oplysningspligten vil ofte være forskellige fra begrundelser for at begrænse indsigtsretten. Tilsvarende vil passende garantier for at beskytte den registreredes interesser afhænge af, om det er oplysningspligten eller indsigtsretten som begrænses.

Begrænsning af ret til indsigt svarende til egenacces i offentlighedsloven (§ 22, stk. 3)

Efter lovforslagets § 22, stk. 3 kan retten til indsigt i oplysninger, der behandles for den offentlige forvaltning,

undtages fra retten til indsigt i samme omfang som efter reglerne i §§ 19-29 og § 35 i offentlighedsloven. Ifølge lovforslagets bemærkninger er bestemmelsen indsat for at sikre, at forvaltningsmyndigheders behandling af personoplysninger kan undtages fra den registreredes ret til indsigt i samme udstrækning som efter offentlighedslovens regler om egenacces, jf. offentlighedslovens § 8. Bestemmelsen svarer til persondatalovens § 32, stk. 2.

Det fremgår af betænkningen side 958, at hvis der for den registrerede er ret til indsigt efter såvel persondataloven som offentlighedsloven, skal afgørelsen træffes på det retsgrundlag, som er mest gunstigt for den pågældende. Men dette princip omtales ikke i bemærkningerne til lovforslaget (databeskyttelsesloven).

På den baggrund finder IT-Politisk Forening det temmelig uklart, om den foreslåede § 22, stk. 3 er ment som en mulighed for at begrænse retten til indsigt, der kan anvendes ved siden af § 22, stk. 1-2, eller om § 22, stk. 3 skal forstås som en indsnævring af mulighederne for at anvende undtagelsesmulighederne i § 22, stk. 1-2, hvis offentlighedslovens regler om egenacces i en konkret sag tillader færre undtagelser fra indsigtsretten end databeskyttelsesforordningen.

IT-Politisk Forening skal opfordre til, at den nærmere sammenhæng mellem § 22, stk. 1-2 og stk. 3 bliver præciseret. Hvis det er meningen, at § 22, stk. 3 tillader undtagelser i situationer, der ikke falder ind under stk. 1-2, skal disse (yderligere) undtagelser have en hjemmel i databeskyttelsesforordningens artikel 23 ligesom undtagelserne efter § 22, stk. 1-2, og dette bør præciseres i lovforslagets bemærkninger.

Begrænsning ret til indsigt i forbindelse med forskning og statistik (§ 22, stk. 5)

Efter lovforslagets § 22, stk. 5 er der ikke ret til indsigt, hvis oplysningerne udelukkende behandles i videnskabeligt øjemed, eller hvis oplysningerne kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker. Bestemmelsen svarer til persondatalovens § 32, stk. 4.

Persondatalovens § 32, stk. 4 er baseret på databeskyttelsesdirektivets artikel 13, stk. 2, som tillader en begrænsning af indsigtsretten under de anførte betingelser. I databeskyttelsesforordningen må adgangen til at begrænse retten til indsigt for personoplysninger der behandles til videnskabelige forskningsformål eller statistiske formål skulle søges i forordningens artikel 89, stk. 2, som tillader en begrænsning af den registreredes rettigheder efter bl.a. artikel 15, såfremt sådanne rettigheder sandsynligvis vil gøre det umuligt eller i alvorlig grad hindre opfyldelse af de specifikke formål, og sådanne undtagelser er nødvendige for at opfylde formålene.

Databeskyttelsesforordningens artikel 89, stk. 2 har altså yderligere betingelser sammenlignet med databeskyttelsesdirektivets artikel 13, stk. 2, som alt andet lige må indsnævre muligheden for at begrænse retten til indsigt. Der vil givetvis være forskningsprojekter, hvor det er relativt uproblematisk at give den registrerede ret til indsigt i egne oplysninger, og i sådanne situationer bør indsigtsretten ikke afskæres. Det samme kunne meget vel gælde personoplysninger, som opbevares hos eksempelvis Danmarks Statistik i personhenførbar form med CPR-numre med henblik på udarbejdelse af statistikker via registersamkøring.

Hvis personoplysningerne er anonymiseret hos en dataansvarlig, som oplysningerne er videregivet til, eksempelvis anonymisering efter udarbejdelse af statistikker som kræver personhenførbare oplysninger til registersamkøring, vil det naturligvis ikke længere være muligt for den dataansvarlige at efterkomme anmodninger om indsigt, jf. også forordningens betragtning 64.

Begrænsning af oplysningspligt ved viderebehandling til andre formål (§ 23)

Lovforslagets § 23 fastsætter en undtagelse fra oplysningspligten efter databeskyttelsesforordningens artikel 13, stk. 3 og artikel 14, stk. 4, hvis personoplysningerne af offentlig myndigheder viderebehandles til et andet formål via en bekendtgørelse udstedt efter databeskyttelseslovens § 5, stk. 3.

Udgangspunktet i forordningen er en fornyet oplysningspligt, hvis personoplysningerne efter indsamling senere viderebehandles til et nyt formål. Men denne pligt til yderligere oplysning ophæves for offentlige myndigheder med lovforslagets § 23.

I bemærkningerne pkt. 2.4.3.5 anfører Justitsministeriet, at det er tvivlsomt om en fornyet oplysningspligt i denne situation reelt vil skabe større retssikkerhed for den registrerede, og at det er administrativt byrdefuldt for den dataansvarlige. IT-Politisk Forening er meget uenig i det første punkt. Efter vores opfattelse har det stor værdi for borgerne at få information om, at deres personoplysninger nu anvendes til andre formål, idet formålsbegrænsningen er et af de helt centrale elementer i beskyttelsen af personoplysninger. Det er også af afgørende betydning for borgernes tillid til offentlige myndigheders forvaltning af deres personoplysninger, at borgerne har mulighed for at få information om anvendelsen af personoplysningerne.

Den generelle begrænsning af oplysningspligten i forbindelse med viderebehandling efter § 5, stk. 3 sker med henvisning til artikel 23, stk. 1, litra e), som omhandler en medlemsstats væsentlige økonomiske interesser. I disse tider, hvor stort set hele befolkningen er tvunget til at modtage digital post fra det offentlige, skulle man umiddelbart mene, at den relevante information kan gives til borgerne uden de store udgifter for den dataansvarlige offentlige myndighed.

Det fremgår ikke af § 23 eller bemærkningerne hertil, om den dataansvarlige skal give information om viderebehandlingen på andre måder end direkte information til den registrerede, for eksempel ved offentliggørelse på den offentlige myndigheds hjemmeside.

Databeskyttelsesforordningens artikel 14, stk. 5, litra c) giver mulighed for at udelade oplysning til den registrerede, hvis indsamlingen eller videregivelsen er udtrykkelig fastsat i medlemsstaternes nationale ret, og at der er fastsat passende foranstaltninger til beskyttelse af den registreredes legitime interesser.

Når Justitsministeriet ikke mener, at 14, stk. 5, litra c) er

tilstrækkelig til at mindske de påståede byrder for den offentlige sektor, og Justitsministeriet derfor søger en begrænsning af oplysningspligten via artikel 23, kan man meget vel frygte, at det heller ikke er meningen, at borgeren skal have udtrykkelig information om viderebehandlingen på anden måde, for eksempel via information på hjemmesider.

Den tyske GDPR-lov tillader i §§ 32-33 under visse (noget mere specifikke) omstændigheder begrænsninger af oplysningspligten ved viderebehandling, men i disse situationer fastsættes der samtidig en klar forpligtelse for den dataansvarlige om at give offentligheden den relevante information i en præcis, transparent, forståelig og let tilgængelig form med et klart og enkelt sprog.

IT-Politisk Forening vil anbefale, at der for at beskytte den registreredes interesser stilles krav til den dataansvarlige om at give offentligheden den relevante information på en præcis, transparent, forståelig og let tilgængelig måde (svarende til kravene i den tyske GDPR-lov), eksempelvis via den dataansvarliges hjemmeside, hvis den individuelle oplysningspligt ved viderebehandling begrænses i henhold til lovforslagets § 5, stk. 3.

Det er ikke tilstrækkeligt, at borgerne blot kan orientere sig i Lovtidende, hvis de er interesseret i at vide hvordan deres personoplysninger viderebehandles og videregives, som Justitsministeriet anfører i pkt. 2.3.4.5 i de almindelige bemærkninger. Antallet af bekendtgørelser, som borgerne i så fald skal læse vil være meget stort, og borgerne kan ikke være sikre på, at den relevante information om hvilke oplysninger, der konkret viderebehandles eller videregives, er udtrykkeligt fastsat i disse bekendtgørelser.

Sanktioner for offentlige myndigheder (§ 41, stk. 5)

Ifølge lovforslaget udestår en stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder til senere. Overvejelser for og imod sanktioner til offentlige myndigheder er heller ikke omtalt i lovforslagets almindelige bemærkninger. Det samme gælder betænkningen, hvor der i forhold til sanktioner over for offentlige myndigheder blot henvises til det kommende lovforslag.

Når Justitsministeren fremsætter lovforslaget om databeskyttelsesloven over for Folketinget, vil IT-Politisk Forening overveje at fremsende et supplerende høringssvar til Retsudvalget. I mellemtiden har vi følgende bemærkninger om sanktionsspørgsmålet i forhold til offentlige myndigheder.

Den nuværende situation for behandlingen af personoplysninger i den offentlige sektor er klart utilfredsstillende. Datatilsynet offentliggør et stort antal udtalelser hvor der konstateres problemer med datasikkerheden hos offentlige myndigheder. Under den gældende persondatalov er Datatilsynets sanktionsmuligheder begrænset til at udtale kritik og offentliggøre udtalelsen på tilsynets hjemmeside. Risikoen for at blive udstillet på denne lidet flatterende måde har haft en bemærkelsesværdig manglende effekt på de offentlige myndigheder. Datatilsynet har offentligt udtalt deres bekymring over den manglende reaktion fra offentlige myndigheder, jf. artiklen ”Datatilsynet: Vi bliver sat skakmat, når myndigheder ignorerer vores kritik”, i netmediet Version2 den 9. august 2017 [2].

Mulighed for bøder til offentlige myndigheder vil give Datatilsynet de effektive reaktionsmuligheder, som mangler i dag. Derudover vil risikoen for bøder også skabe et direkte økonomisk incitament hos offentlige myndigheder til at overholde databeskyttelses-forordningen. Det kan samtidig modvirke eventuelle incitamenter til at spare så meget på IT-sikkerheden, at det bliver vanskelige eller direkte umuligt for den offentlige myndighed at overholde kravene i databeskyttelses-forordningen.

Det er også krænkende for den almindelige retsbevidsthed, at offentlige myndigheder uden konsekvens kan overtræde databeskyttelsesreglerne, specielt når der samtidig sker en væsentlig skærpelse af sanktionerne over for private aktører.

Tilsynsmyndighedernes mulighed for at anlægge en sag for at annullere en tilstrækkelighedsvurdering

Det fremgår af EU-Domstolens præmis 65 i Schrems-sagen

C-362/14, at medlemsstaternes nationale ret skal indeholde mulighed for at tilsynsmyndigheden kan anlægge en sag ved de nationale domstole, hvis tilsynsmyndigheden mener at en klage over en tilstrækkelighedsvurdering fra Kommissionen er begrundet. Hvis den nationale domstol er enig med tilsynsmyndigheden, skal spørgsmålet forelægges EU-Domstolen til præjudiciel afgørelse, idet EU-Domstolen er den eneste domstol i Unionen, som har kompetence til at fastslå, at en afgørelse fra Kommissionen er ugyldig.

Det specielle ved denne situation er at tilsynsmyndigheden skal anlægge en retssag uden at have en modpart (hvis tilsynsmyndigheden ikke er enig med klageren, kan klageren anlægge en sag mod tilsynsmyndigheden på normal vis, og fra denne sag kan der, hvis den nationale domstol er enig med klageren, komme en præjudiciel forelæggelse for EU-Domstolen).

Den tyske GDPR-lov indeholder i § 21 en særlig beføjelse for tilsynsmyndigheden til anlægge en sag uden modpart med henblik på eventuelt at foreligge spørgsmålet om gyldigheden af en tilstrækkelighedsvurdering for EU-Domstolen.

Muligheden for at Datatilsynet kan anlægge en sådan sag ved danske domstole, i overensstemmelse med præmis 65 i C-362/14, er ikke omtalt i lovforslagets bemærkninger. IT-Politisk Forening kan ikke vurdere, om Datatilsynet allerede har denne mulighed efter gældende ret, eller om det vil kræve en passende særregel for at Datatilsynet kan indbringe en sådan sag for domstolene.

Noter

[1] Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680, Federal Ministry of the Interior http://www.bmi.bund.de/SharedDocs/Downloads/EN/Gesetzestexte/datenschutzanpassungsumsetzungsgesetz.htm

[2] ”Datatilsynet: Vi bliver sat skakmat, når myndigheder ignorerer vores kritik”, Version2, 9. august 2017 https://www.version2.dk/artikel/datatilsynet-vi-bliver-sat-skakmat-naar-myndigheder-ignorere-vores-kritik-1078928

Justitsministeriet
databeskyttelseskontoret@jm.dk

KL's høringssvar til databeskyttelsesloven

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Ved mail af 7. juli 2017 har Justitsministeriet anmodet KL om at give eventuelle bemærkninger til udkast til databeskyttelsesloven.

KL har gennemgået det fremsendt udkast til databeskyttelsesloven med fokus de emner, der har særlig betydning for kommunerne, og har målrettet kommenteringen til disse.

Ny version af den danske "krigsregel", § 3, stk. 9

Der er i lovforslaget stillet forslag om, at personoplysninger i nogle tilfælde kun må opbevares i Danmark. Det kan reelt kan betyde, at offentlige myndigheder i mange tilfælde ikke kan anvende billigste leverandør og effektive og billige cloud-løsninger. KL finder, at der i stedet bør overvejes andre løsningsmodeller, der på samme vis kan sikre statens sikkerhed. KL indgår gerne i drøftelser af alternative muligheder.

Det er KL´s vurdering, at lovforslagets krav om, at personoplysninger der behandles i offentlige it-systemer i nogle tilfælde alene må opbevares i Danmark af hensyn til statens sikkerhed, giver flere problemer for kommunerne og ikke er en tidssvarende model for sikring af data.

Først og fremmest vil kravet have økonomiske konsekvenser, da kommunerne ikke vil kunne anvende billigere leverandører uden for landets grænser til opbevaring af data.

Herudover vil bestemmelsen betyde, at kommunerne ikke vil kunne anvende cloud-løsninger til opbevaring af data, hvorfor bestemmelsen direkte vil modarbejde intentionerne i den fællesoffentlige digitaliseringsstrategi 2016-2020, "Et stærkere og mere trygt digitalt samfund", hvor af det fremgår, at *"Der vil de kommende år være fokus på at skabe mere konkurrence på markedet for offentlige it-løsninger og reducere myndighedernes omkostninger til it-drift. Der skal derfor åbnes op og skabes klare rammebetingelser for, at myndighederne i højere grad kan benytte hele spektret af it-løsninger, herunder cloud computing. For de offentlige myndigheder vil bedre muligheder for brug af cloud computing på relevante områder betyde, at de kan indkøbe standardiserede og fleksible it-løsninger, der fx giver mulighed for hurtig op- og nedskalering af kapaciteten efter forbrug og behov. Det kan reducere kødannelse, når mange borgere på samme tid ønsker at logge ind på en given tjeneste. For myn-*

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

dighederne kan cloud computing på de rette områder og med blik for sikkerhedsmæssige hensyn dermed give en øget teknisk og forretningsmæssig fleksibilitet samt billigere og mere effektive it-løsninger."

Hertil vurderer KL, at bestemmelsen ikke nødvendigvis vil have den ønskede effekt, eftersom personoplysningerne i de givne it-systemer ofte vil have karakter af grunddata, der anvendes – og dermed vil kunne tilgås – via mange andre offentlige, herunder kommunale, systemer.

KL er derfor samlet set enig i betragtningerne i betænkningen om databeskyttelsesforordningen (nr. 1565), hvoraf det fremgår, at "*Der er således sket en betydelig teknologisk udvikling siden vedtagelsen af persondataloven i 2000, hvorefter den fysiske driftsafvikling af et system inden for Danmarks grænser ikke nødvendigvis længere er en garanti for at sikre bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold. Kravet om at sikre bortskaffelse eller tilintetgørelse af de oplysninger, der er indeholdt i registrene vil således måske kunne ske ved at anvende en anden sikkerhedsmodel."* (s. 550).

Viderebehandling/genanvendelse af data, § 5

Der er i lovforslaget stillet forslag om, at offentlige myndigheders genanvendelse af personoplysninger kan ske ved, at den enkelte ressortminister på konkrete områder fastsætter regler om dette. KL finder, at denne model ikke med tilstrækkelig hastighed vil understøtte myndighedernes muligheder for at anvende teknologi og data til at udvikle den kommunale service og sikre borgerne bedre og lettere kontakt med myndighederne. KL mener, at der i stedet bør indsættes en generel, national hjemmel til offentlige myndigheders genanvendelse af personoplysninger i databeskyttelsesloven.

De retlige rammer bør ikke spænde ben for kommunernes (og øvrige myndigheders) muligheder for at anvende teknologi og (gen)bruge data til at udvikle den kommunale service til gavn for borgerne. Det er et hensyn, som KL er enig med regeringen i, og som derfor er et væsentligt indsatsområde i den fællesoffentlige digitaliseringsstrategi, hvor der bl.a. er en målsætning om, at borgeren ikke skal bruge tid på at aflevere data til de offentlige myndigheder, som myndighederne allerede er i besiddelse af.

I lovforslagets § 5, stk. 1 og 2, er databeskyttelsesforordningens regler for genanvendelse/viderebehandling af personoplysninger til nye formål gentaget. Herefter er udgangspunktet, at personoplysninger ikke må genanvendes, såfremt de nye behandlinger af data er "uforenelige" med det oprindelige indsamlingsformål. I sit udgangspunkt er det ikke en retlig ramme, der understøtter genbrug af data.

Efter stk. 2 åbnes der op for, at der lovligt vil kunne ske genanvendelse af én gang indsamlede oplysninger om borgerne til nye formål, såfremt formålene ud fra en konkret vurdering må anses at være forenelige med det oprindelige formål. For kommunerne vil det ikke skabe nogen effektivisering og bedre udnyttelse af data, såfremt hver enkelt genanvendelse

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

skal underkastes en konkret vurdering, den såkaldte "ikke-uforenelighedstest". Effektiv genanvendelse af personoplysninger sker typisk automatisk via digitale løsninger, der udveksler allerede indsamlede data.

I lovforslagets § 5, stk. 3, er muligheden i databeskyttelsesforordningens artikel 6, stk. 4, for at fastsætte national regulering, der tillader genanvendelse af personoplysninger til formål, der er uforenelige med de oprindelige indsamlingsformål, udnyttet. Dette finder KL finder positivt og nødvendigt. Imidlertid er bestemmelsen udformet som en delegationsbestemmelse, hvorefter hver enkelt minister på hver deres ressortområde skal vurdere behovet for nærmere regler om genanvendelse af personoplysninger. KL´s finder denne model tung og langsommelig i forhold til hurtigst muligt at sikre digitaliseringsklar lovgivning, der understøtter udnyttelse af de digitale muligheder.

Samkøring i kontroløjemed

KL ser med tilfredshed, at det med lovforslaget ikke længere vil være et krav, at samkøring af personoplysninger i kontroløjemed skal have særskilt lovhjemmel. Dette vil betyde administrative lettelser for kommunerne set i sammenhæng med, at databeskyttelsesforordningen heller ikke stiller krav om, at kommunerne skal indhente Datatilsynets tilladelse til samkøring i kontroløjemed, eller at der skal gives information til de registrerede, inden samkøringen foretages.

KL er enig med Justitsministeriet i, at databeskyttelsesforordningens artikel 5 og artikel 6, stk. 4, om principper for behandling af personoplysninger, herunder proportionalitetsprincippet og princippet om formålsbegrænsning, yder en tilstrækkelig stærk beskyttelse til de registrerede samtidig med, at forordningens sikrer rum for offentlige myndigheders saglige behov for at kunne samkøre personoplysninger i kontroløjemed.

Behandling af følsomme oplysninger, § 7

I forhold til lovforslagets § 7 ser KL med tilfredshed, at oplysninger om væsentlige sociale problemer og andre rent private forhold ikke er medtaget i bestemmelsen, men at disse oplysninger alene reguleres af databeskyttelsesforordningens artikel 6.

KL ser endvidere med tilfredshed, at den nuværende § 13 i persondataloven ikke er opretholdt i lovforslaget, og vil gerne kvittere for denne regelforenkling.

Behandling af følsomme oplysninger, § 7, stk. 2-3

KL har med tilfredshed noteret sig, at Justitsministeriet i forslagets § 7, stk. 2, har udnyttet muligheden for at fastsætte en national regel i henhold til forordningens artikel 9, stk. 2, litra b, som muliggør behandling af følsomme personoplysninger, hvis det er nødvendigt for at overholde den dataansvarliges eller den registreredes arbejdsretlige forpligtelser og specifikke rettigheder.

KL har ligeledes med tilfredshed noteret sig, at det af afsnit 2.3.3.3., side 183, fremgår, at baggrunden for fastsættelsen af reglen i § 7, stk. 2, er en

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

tanke om, at det skal være muligt at behandle følsomme oplysninger i samme omfang som efter den nugældende persondatalov.

I forlængelse heraf bemærkes, at KL tidligere har efterspurgt en afklaring af, hvad der ligger i artikel 9, stk. 2, litra b's krav om "*fornødne garantier for den registreredes grundlæggende rettigheder og interesser*". KL har derfor med tilfredshed noteret sig, at der i afsnit 2.3.3.3., side 184-185, er anført en række eksempler på foranstaltninger, som den dataansvarlige kan iværksætte med henblik på at overholde artikel 9, stk. 2, litra b.

Det bemærkes i øvrigt, at formuleringen af bemærkningerne til § 7, stk. 2, desværre kan give anledning til nogen forvirring om, hvilken type personoplysninger bestemmelsen i § 7, stk. 2, omfatter. Bestemmelsen er formuleret sådan, at den omfatter alle typer følsomme oplysninger omfattet af forordningens artikel 9, stk. 1. Bemærkningerne side 265, midt, er imidlertid formuleret sådan, at man kunne forledes til at tro, at bestemmelsen i § 7, stk. 2, kun omfatter oplysninger om fagforeningsmæssige tilhørsforhold. KL skal opfordre til, at denne uklarhed rettes op.

KL har i øvrigt noteret sig, at Justitsministeriet ikke har ønsket fuldt ud at udnytte muligheden for at indføre nationale regler i henhold til forordningens artikel 9, stk. 2, litra h, idet bl.a. "*arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne*" ikke er omfattet af forslagets § 7, stk. 3. KL har dog samtidig noteret sig, at det i bemærkningerne til § 7, side 266, er anført, at det kan være vanskeligt på forhånd fuldstændigt at forudse behovet for at kunne behandle personoplysninger omfattet af forordningens artikel 9, stk. 1, og at der i stk. 5 derfor foreslås indført en bemyndigelse for vedkommende minister til – efter forhandling med justitsministeren og inden for forordningens rammer - at fastsætte yderligere regler om lovlig behandling af personoplysninger omfattet af artikel 9, stk. 1.

Strafbare forhold, § 8

Den danske særregel i den nuværende persondatalovs § 8 foreslås opretholdt i forslag til databeskyttelseslovens § 8 for så vidt angår oplysninger om strafbare forhold. Af hensyn til regelforenkling og minimering af de administrative byrder er det KL's opfattelse, at § 8 i forslag til databeskyttelsesloven bør udgå. De øvrige behandlingsbestemmelser i databeskyttelsesforordningen og forslag til databeskyttelsesloven findes at være tilstrækkelige i forbindelse med behandling af strafbare forhold.

Det følger af databeskyttelsesforordningens artikel 10, 1. pkt., at behandlingsgrundlaget for oplysninger om strafbare forhold for offentlige myndigheder er artikel 6, stk. 1, om almindelige personoplysninger.

Det fremgår af de almindelige bemærkninger til lovforslaget afsnit 2.3.4.2., at det antages, at den danske særregel i persondatalovens § 8 kan opretholdes på baggrund af databeskyttelsesforordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2 og 3.

Der er således ikke i databeskyttelsesforordningen en forpligtelse til at videreføre den danske særregel i den nuværende persondatalovs § 8.

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Det er KL's opfattelse, at behandlingsreglen i den nuværende persondatalovs § 8 i praksis har givet anledning til fortolkningstvivl og opfattes som en yderligere kompleksitet i sagsbehandlingen.

Anvendelse af statistikdata, § 10

Lovforslaget gør det ikke muligt for kommunerne at genanvende de oplysninger om borgerne, som eventuelt afdækkes ved statistik. Anvendelse af statistik er for kommunerne et vigtigt element i at kunne tilbyde den bedst mulige service og hjælp til borgerne. KL finder derfor, at der i databeskyttelsesloven bør etableres mulighed for dette – på samme måde som det i lovforslaget foreslås muligt på sundhedsområdet.

Kommunerne anvender i høj grad statistik med henblik på at kunne levere den bedst mulige service og hjælp til borgerne. Når kommunerne udarbejder statistik på baggrund af oplysninger om borgere, kan det bl.a. være for at søge at afdække, om der er borgere, der kan have brug for anden eller yderligere hjælp. Kommunerne har derfor et ønske om at kunne anvende disse oplysninger om borgerne til at træffe nye foranstaltninger eller afgørelser vedrørende bestemte personer med henblik på at give disse borgere en bedre hjælp eller service.

Formålsbegrænsningen i den foreslåede § 10, stk. 2, gør imidlertid ikke denne anvendelse af oplysningerne mulig. KL vil derfor foreslå, at etableres en særskilt undtagelse fra formålsbegrænsningen for det kommunale område tilsvarende forslagets stk. 5, der er rettet specifikt mod sundhedsområdet.

Det er KL´s vurdering, at de hensyn, der ligger til grund for stk. 5 – varetagelsen af registreredes vitale interesser – også gør sig gældende for kommunernes ydelse af hjælp til borgerne. Kommunerne vil på baggrund af statistik om leverede ydelser kunne blive opmærksomme på ikke tidligere erfarede fysiske, psykiske eller sociale problemer hos enkelte borgere, som kræver valg af ny eller yderligere skræddersyet hjælp til de pågældende borgere.

Behandling af personoplysninger i forbindelse med ansættelsesforhold, § 12

KL har tidligere anmodet om, at Justitsministeriet udarbejder en vejledning om behandling af personoplysninger i forbindelse med ansættelsesforhold. KL fastholder ønsket om en sådan vejledning, der kan bidrage med en enkel og samlet fremstilling af retsstillingen på ansættelsesområdet, og påpeger, at der er behov for, at vejledningen udarbejdes forud for forordningens ikrafttræden den 25. maj 2018 og meget gerne inden december 2017, hvor der er kravsudveksling i forbindelse med overenskomstfornyelse på det kommunale **område, som omfatter ca. 500.000 ansatte.**

Det er i afsnit 2.3.8.3, side 196, anført, at arbejdsgivere i det offentlige ikke længere efter den 25. maj 2018, hvorfra forordningen skal anvendes, kan benytte sig af "interesseafvejningsreglen" i forordningens artikel 6, stk. 1, litra f. Denne bestemmelse svarer til persondatalovens § 6, stk. 1,

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

nr. 7, som hidtil i vidt omfang har været anvendt som behandlingshjemmel af offentlige (og private) arbejdsgivere.

KL er særligt i lyset heraf tilfredse med, at Justitsministeriet med lovforslagets § 12 har foreslået en supplerende hjemmelsbestemmelse, der har til hensigt at bringe fuldstændig sikkerhed for, at der på det offentlige (og private) arbejdsmarked lovligt kan behandles personoplysninger før, under og efter ansættelsesforholdet i samme omfang som hidtil, jf. bemærkningerne til § 12, side 275. Ifølge afsnit 2.3.8.3, side 196, kan der således efter forslagets § 12 behandles personoplysninger på baggrund af kollektive overenskomster, både hvor overenskomsten foreskriver en pligt til behandlingen, og hvor overenskomsten giver mulighed for eller forudsætter behandling af personoplysninger.

KL er ligeledes tilfredse med, at det både i bemærkningerne til § 12, side 275, og i betænkningen side 140 er understreget, at offentlige myndigheder fremover må kunne anvende artikel 6, stk. 1, litra e, som behandlingshjemmel, når de behandler personoplysninger som arbejdsgiver. KL skal dog opfordre til, at der i lovbemærkningerne anføres eksempler på, hvornår artikel 6, stk. 1, litra e, kan tænkes anvendt af offentlige arbejdsgivere. Der tænkes her særligt på behandlinger, hvor man tidligere ville have anvendt "interessevejningsreglen" i persondatalovens § 6, stk. 1, nr. 7, som hjemmel, og som ikke er omfattet af den foreslåede bestemmelse i lovforslagets § 12, dvs. behandlinger som ikke er fastlagt i eller udspringer af anden lovgivning eller kollektive overenskomster. Det kunne fx være offentliggørelse af arbejdsrelaterede medarbejderoplysninger på hjemmesider, anvendelse af medarbejderfotos i en intern telefonbog, orientering af øvrige medarbejdere på arbejdspladsen om at en medarbejder er fratrådt, eller anvendelse af en medarbejders mailadresse i en vis periode efter medarbejderens fratræden.

I forlængelse heraf skal KL også opfordre til, at der i bemærkningerne til lovforslagets § 12, stk. 2, side 276, anføres eksempler på, hvilke behandlinger der tænkes omfattet af denne bestemmelse.

KL har tidligere efterspurgt afklaring af, om samtykke fremadrettet kan anvendes som grundlag for behandling af personoplysninger i forbindelse med ansættelsesforhold. KL er derfor tilfreds med, at det med lovforslagets § 12, stk. 3, er slået fast, at samtykke også kan anvendes som behandlingsgrundlag før, under og efter ansættelse. KL skal dog opfordre til, at der i bemærkningerne til bestemmelsen anføres noget uddybende vedrørende bestemmelsens henvisning til forordningens artikel 7, herunder særligt artikel 7, stk. 4. KL henleder i den forbindelse opmærksomheden på, at Artikel 29-gruppen den 8. juni 2017 har udsendt en udtalelse (2/2017) om bl.a. muligheden for at anvende samtykke som behandlingsgrundlag i ansættelsesforhold. Artikel 29-gruppen konkluderer i udtalelsen bl.a. følgende (afsnit 6.2, side 23): "*Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free concent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer.*" Artikel 29-gruppens fortolkning er såle-

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

des mere snæver end § 12, stk. 3, i lovforslaget. Det skaber en uhensigtsmæssig usikkerhed om muligheden for at bruge den foreslåede hjemmel i lovforslagets § 12, stk. 3, om anvendelse af samtykke i ansættelsesforhold.

Det fremgår af afsnit 2.3.8.3, side 197, at den foreslåede bestemmelse i § 12 har sin baggrund i forordningens artikel 88, og at der ikke er tvivl om, at der kan fastsættes nationale behandlingsregler i love og kollektive overenskomster for så vidt angår behandling af alle typer oplysninger – under overholdelse af kravene til sådan national lovgivning i fx artikel 9, stk. 2, og artikel 88, stk. 2. Det er også anført, at de kollektive overenskomster, der danner baggrund for behandling efter lovforslagets § 12, skal leve op til kravene hertil efter artikel 88, stk. 2.

Forordningens artikel 9, stk. 2, litra b, og artikel 88, stk. 2, stiller krav om henholdsvis "*fornødne garantier for den registreredes grundlæggende rettigheder og interesser*" og "*passende og specifikke foranstaltninger til beskyttelse af den registreredes menneskelige værdighed, legitime interesser og grundlæggende rettigheder*". KL opfordrer til, at indholdet af disse krav beskrives nærmere i lovforslagets bemærkninger til § 12, sådan som det også er sket for så vidt angår lovforslagets § 7, stk. 2, som bygger på forordningens artikel 9, stk. 2, litra b (afsnit 2.3.3.3., side 184-185).

Databeskyttelsesloven og arkivloven, § 14

Med § 14 videreføres de gældende regler om, at personoplysninger omfattet af persondataloven vil kunne arkiveres efter arkivlovens regler. For at øge klarheden overfor borgere og administrerbarheden foreslår KL, at der fastlægges nærmere regler om behandling af personoplysninger i offentlige arkiver og kriterier for adgang og tilgængeliggørelse efter udløb af tilgængelighedsfrister.

KL skal gøre opmærksom på, at det ikke efter de gældende regler er fuldstændig entydigt, i hvilket omfang personoplysninger, der er afleveret til et offentligt arkiv, efter udløb af tilgængelighedsfrister, alene er omfattet af arkivloven, eller hvordan persondatalovens bestemmelser fortsat skal iagttages ved arkivmæssig behandling, fx tilgængeliggørelse på internettet.

Med en uændret videreførelse af bestemmelserne i databeskyttelsesloven vil denne usikkerhed fortsat kunne bestå, ifm. offentlige arkivers behandling af ansøgninger om adgang til og behandling af arkivalier. Pga. uklarheden i den nuværende lovgivning, bliver forvaltningen af arkivområdet i nogle tilfælde unødigt kompliceret.

Fornyet oplysningspligt, § 23

I forhold til § 23 i forslag til databeskyttelseslov har KL noteret sig, at den fornyede oplysningspligt i databeskyttelsesforordningens artikel 13, stk. 3 og 14, stk. 4, ikke finder anvendelse, når offentlige myndigheder viderebehandler personoplysninger til et andet formål end det, hvortil de er indsamlet. Det fremgår af de almindelige bemærkninger til lovforslaget afsnit

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

2.4.3.5., at den fornyede oplysningspligt vil opleves som administrativ byrdefuld for den dataansvarlige, og at det samtidig vil være tvivlsomt om en fornyet oplysningspligt reelt vil skabe en større retssikkerhed for den registrerede. KL ser med tilfredshed, at denne udvidelse af oplysningspligten, som for kommunerne ville være administrativ byrdefuld, ikke er medtaget i lovforslaget.

Ret til erstatning, § 40
Det er i afsnit 2.8.1.3, side 235, og afsnit 2.8.3.5, side 244, vedrørende gældende ret efter persondatalovens § 69 bl.a. nævnt, at der er tale om et præsumptionsansvar (culpa med omvendt bevisbyrde), og at erstatningsansvaret i øvrigt reguleres af de almindelige erstatningsretlige principper.

Det fremgår af afsnittene henholdsvis om forordningens artikel 82 (afsnit 2.8.2.4, side 237) og om Justitsministeriet overvejelser herom (afsnit 2.8.3.5, side 244) samt af bemærkningerne til lovforslagets § 40 (side 317), at der også fremadrettet gælder et præsumptionsansvar (culpa med omvendt bevisbyrde).

Det er imidlertid ikke i de pågældende afsnit anført, at erstatningsansvaret – ligesom i dag - i øvrigt reguleres af de almindelige erstatningsretlige principper. KL finder, at dette bør tilføjes fx i bemærkningerne til lovforslagets § 40 med henblik på at øge klarheden om retstilstanden.

Bøder, § 41

Det fremgår af lovforslagets § 41, stk. 5, at stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder udestår. Spørgsmålet om bøder, der som straf for overtrædelse af reglerne idømmes ved domstolene til offentlige myndigheder, har naturligvis stor interesse for KL og stor betydning for kommunerne og den kommunale økonomi. KL er enig i, at det er vigtigt at sikre beskyttelse af persondata, og at også kommunerne selvsagt har et ansvar for, at dette sker. Det er imidlertid KL's opfattelse, at bøder ikke er hensigtsmæssig for offentlige myndigheder, men at andre instrumenter som skærpet tilsyn fra Datatilsynet, indberetning om sikkerhedsbrud og udpegning af en databeskyttelsesrådgiver er langt mere effektive.

KL ønsker at påpege, at der også her er grundlæggende forskel på private og offentlige aktører, og at aktørerne som udgangspunkt er reguleret forskelligt både i øvrig regulering og i andre dele af databeskyttelsesforordningen. Derfor ønsker KL at henlede opmærksomheden på, at offentlige myndigheder – såvel medarbejdere, ledere som politikere i forvejen er reguleret tæt, hvis myndigheden ikke overholder gældende regler. Dette gælder ikke i nær samme omfang for private aktører, der er reguleret anderledes. Af disse grunde finder KL det ikke hensigtsmæssigt, at der arbejdes med indførelse af store økonomiske sanktioner til offentlige myndigheder.

Offentlige myndigheder er ved lov pålagt at udføre bestemte opgaver. Hvis en kommune pålægges en meget stor bøde, kan kommunen ikke stoppe med at udføre sine opgaver. Det vil betyde, at kommunen skal

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

skære i den service, som kommunen leverer, på fx skoler eller i ældreplejen. De bevillingsretlige rammer giver ikke myndighederne andre muligheder for at finansiere bøderne.

Det er KL's opfattelse, at vi i Danmark allerede har en række strafbestemmelser/sanktioner, som vil udgøre en effektiv håndhævelse af databeskyttelsesforordningen for offentlige myndigheder:

- Offentligt ansatte kan allerede i dag blive straffet efter straffelovens § 152, hvis de uberettiget videregiver eller udnytter fortrolige oplysninger om borgerne, som de har fået adgang til via deres arbejde.

- Datatilsynet kan i dag efter persondataloven udtale kritik af myndighederne, hvis de ikke overholder reglerne om databeskyttelse. Det er kritik, der tages meget alvorligt i kommunerne. En offentliggørelse af kritik eller problemer med datasikkerhed opleves som "straf" nok. De kommuner, som har været udsat for kritik, har "rettet ind" efterfølgende og sat større opfølgninger i gang.

- Efter de nye regler i databeskyttelsesforordningen bliver myndighederne forpligtede til at indberette eventuelle sikkerhedsbrud til Datatilsynet, sådan at Datatilsynet kan kontrollere, at myndighederne i tilstrækkeligt omfang afhjælper konsekvenserne af sikkerhedsbrud.

- Databeskyttelsesforordningens krav om, at offentlige myndigheder – til forskel fra private virksomheder – altid er forpligtede til at udpege en databeskyttelsesrådgiver er et nyt og vigtigt tiltag, som vil medvirke til at sikre, at kommunerne lever op til reglerne i databeskyttelsesforordningen. Opmærksomheden henledes her på, at databeskyttelsesrådgiveren rapporterer direkte til kommunalbestyrelsen. Kommunalbestyrelsen får således fremover en viden om kommunens arbejde med persondata, og dermed et grundlag for at handle i forhold til at sikre den krævede beskyttelse af borgernes persondata.

- Det kommunale tilsyn kan efter kommunestyrelsesloven pålægge medlemmer af kommunalbestyrelserne tvangsbøder, hvis den enkelte kommune ikke udfører de pligter, som kommunen er pålagt, fx efter databeskyttelsesforordningen. Det kan være daglige bøder, hvis der er behov for det. Det er det enkelte medlem, der selv skal betale en sådan tvangsbøde.

Hertil kommer, at der er iværksat en række awareness-aktiviteter, som undervisning og kampagner med fokus på sikkerhed, hvor pengene bruges på reel øget sikkerhed. Dette samarbejdes der allerede om mellem stat, regioner og kommuner, og indsatsen er aftalt intensiveret i den fælles offentlige digitaliseringsstrategi.

Derudover finder KL, at det skærpede tilsyn fra Datatilsynet (som der er lagt op til i databeskyttelsesforordningen), vil kunne understøtte et øget fokus på forebyggelse og sikkerhed, såfremt tilsynet har karakter af at

være et kvalitetsudviklende tilsyn, hvor tilsynet, udover at stille krav om dokumentation for at kommunen har rettet "fejlen", også indgår i dialog med kommunen om at iværksætte de fornødne initiativer til at forebygge gentagelser.

Hvis man på trods af ovenstående ønsker at kunne pålægge kommunerne bøder, bør man se på, om eventuelle overtrædelser reelt betyder kompromittering af borgernes data. En række af databeskyttelsesreglerne er administrative krav, hvor manglende overholdelse ikke i sig selv berører borgeren (fx krav om at føre fortegnelser over kommunens behandlinger af persondata).

Konsekvenserne af persondatalovens ophævelse, § 46

Når persondataloven ophæves den 25. maj 2018 bortfalder samtlige bekendtgørelser og vejledninger udstedt med hjemmel i loven. Særligt på sikkerhedsområdet har dette store konsekvenser for kommunerne, da sikkerhedsbekendtgørelsen og tilhørende vejledning bortfalder uden, at databeskyttelsesforordningen giver mulighed for, at der nationalt kan udarbejdes en ny, national sikkerhedsbekendtgørelse til de offentlige myndigheder. KL finder det derfor af største vigtighed, at Justitsministeriet sikrer tilstrækkelig vejledning i en tid, hvor krav til og fokus på sikkerhed øges.

Databeskyttelsesforordningen giver i sig selv ikke megen specifik hjælp til, hvilke sikkerhedsforanstaltninger der vil blive stillet krav om hos kommunerne. KL vil derfor benytte lejligheden til at påpege vigtigheden af, at den vejledning om behandlingssikkerhed, som Justitsministeriet vil offentliggøre i december 2017, bliver så konkret i sin vejledning som muligt.

Konsekvensanalyser vedrørende databeskyttelse

Af hensyn til de store økonomiske konsekvenser for kommunerne, finder KL det nødvendigt, at udarbejdelsen af konsekvensanalyser i forbindelse med ministeriernes udarbejdelse af lovforslag bliver eksplicit omtalt i databeskyttelsesloven.

Kommunerne bliver med databeskyttelsesforordningen pålagt en ny administrativ opgave, idet kommunerne bliver forpligtede til at udarbejde såkaldte konsekvensanalyser – analyser af behandlinger af persondatas konsekvenser for databeskyttelsen, jf. forordningens artikel 35.

Analyserne skal bl.a. udarbejdes, når kommunerne via ny lovgivning bliver forpligtede til behandlinger af persondata, der kan karakteriseres som værende af "høj risiko", hvilket bl.a. vil være tilfældet, når kommunerne forpligtes til at udføre behandlinger i stort omfang af følsomme data om borgerne, som det ofte er tilfældet i den kommunale sektor.

For kommunerne vil den nye opgave få administrative og økonomiske konsekvenser, idet det at udarbejde konsekvensanalyser er en større opgave, der kræver mange ressourcer, og også er en opgave, der kræver særlige kompetencer, så der vil blive behov for kompetenceudvikling af de relevante kommunale medarbejdere.

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Databeskyttelsesforordningen giver imidlertid mulighed for at effektivisere arbejdet med udarbejdelsen af disse konsekvensanalyser, idet artikel 35, stk. 10, hjemler adgang til, at disse konsekvensanalyser kan udarbejdes "en gang for alle" i forbindelse med udarbejdelsen af det pågældende, nationale lovgrundlag, som ligger til grund for de kommunale behandlinger af persondata.

Da dette effektiviseringstilgang vil spare kommunerne for store (konsulent)udgifter til udarbejdelse af analyserne, har KL i forbindelse med høringen af Udkast til Vejledning om lovkvalitet anbefalet, at vejledningen om lovkvalitet eksplicit medtager et afsnit om udarbejdelse af disse analyser. Sådan at udarbejdelsen af konsekvensanalyser bliver en opgave på linje med beregningen af de økonomiske, administrative og miljømæssige konsekvenser af et lovforslag. KL vil anbefale, at dette også fremgår af databeskyttelsesloven.

De økonomiske konsekvenser af implementeringen af databeskyttelsesforordningen

Det er KL's vurdering, at implementeringen af databeskyttelsesforordningen, herunder forslaget til databeskyttelsesloven, vil være forbundet med væsentlige merudgifter for kommunerne. KL ønsker derfor en drøftelse om kompensation i forbindelse med den endelige afklaring af øgede forpligtelser for kommunerne som følge af databeskyttelsesforordningen.

Det drejer sig særligt om forordningens nye administrative krav om:

- øget oplysningspligt (artikel 13 og 14)
- evt. dataportabilitet (artikel 20)
- evt. den dataansvarliges ansvar (artikel 24)
- evt. kravene om databeskyttelse gennem design og standardindstillinger (artikel 25)
- uddybende databehandleraftaler (artikel 28)
- fortegnelseskrav (artikel 30)
- evt. øgede sikkerhedskrav (artikel 32)
- anmeldelse af sikkerhedsbrud (artikel 33)
- underretning om sikkerhedsbrud til den registrerede (artikel 34)
- krav om udarbejdelse af konsekvensanalyser (artikel 35)
- krav om udpegning af en databeskyttelsesrådgiver (artikel 37), herunder kompetencekrav til denne (artikel 37 og 39)

Hertil kommer øgede udgifter til driftsafvikling af it-systemer som følge af forslaget til databeskyttelsesloven § 3, stk. 9, (ny krigsregel).

KL indgår gerne i yderligere dialog om databeskyttelsesloven, og såfremt Justitsministeriet finder, at der er behov for uddybninger af KL's bemærkninger til lovforslaget, står KL til rådighed for dette.

Med venlig hilsen

Laila Kildesgaard

Kristian Heunicke

Dato: 24. august 2017

Sags ID: SAG-2017-03399
Dok. ID: 2381426

E-mail: BIB@kl.dk
Direkte: 3370 3481

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

KOMMUNERNES OG REGIONERNES LØNDATAKONTOR TLF. 33 70 33 70 WWW.KRL.DK
WEIDEKAMPSGADE 10 POSTBOKS 3370 2300 KØBENHAVN S KRL@KRL.DK

Justitsministeriet
Databeskyttelseskontoret@jm.dk

KRL's bemærkninger til forslag til databeskyttelsesloven

Den 22.08.2017

Sagsid.: #1479

Ref kjj

kjj@krl.dk

Dir. 3370 3810

Det Kommunale og Regionale Løndatakontor (KRL) er blevet opmærksom på, at der er udsendt et forslag til en databeskyttelseslov, samt at der er høringsfrist på lovforslaget i dag d. 22. august.

Hvem er KRL:
KRL er en selvejende institution under Økonomi- og Indenrigsministeriet.

KRL's formål er at producere og formidle statistik om løn- og personaleforhold m.v. på det kommunale og regionale område bl.a. til brug for overenskomstforhandlinger m.v. samt – i samarbejde med udbyderne af lønanvisningssystemer m.v. samt statslige og kommunale myndigheder – at forestå udvikling og vedligeholdelse af datagrundlaget for produktion af statistikker.

KRL har endvidere til formål at udvikle og vedligeholde et system af beregningsprogrammer og foretage beregninger i forbindelse med overenskomstforhandlinger m.v.

KRL producerer løn- personale- og fraværsstatistikker på baggrund af de indberettede oplysninger fra kommuner og regioner, indeholdende detaljerede ansættelsesoplysninger om de ansatte i regioner og kommuner inkl. cpr-nummer, detaljerede lønoplysninger, detaljerede oplysninger om arbejdssteder og arbejdstid samt fraværsoplysninger inkl. årsager, hvor alle oplysningerne ligger på individniveau.

En del af de statistikker KRL udarbejder udarbejdes ligeledes som tidsserier, hvorfor det er væsentlig for KRL ikke blot at modtage alle oplysningerne på individniveau, men ligeledes at have mulighed for at opbevare data i en meget lang periode til brug for tidsserierne.

KRL stiller datagrundlaget til rådighed Kommuner og regioner, Danmarks Statistik og andre statsmyndigheder, der har hjemmel til at få løn- og personalestatistiske data fra kommuner og regioner, Den kommunale sektors lønforhandlende organ (KL) samt Regionernes Lønnings- og Takstnævn. KRL offentliggør løbende statistikker på deres hjemmeside som alle har adgang til.

KRL stiller endvidere datagrundlaget til rådighed for forskere til brug for videnskabelige formål, hvoraf en del af forskerne ligeledes er interesseret i

forløbsanalyser, hvorfor det er nødvendigt at opbevare grunddata i en meget lang periode.

KRL's datagrundlag ligger ligeledes til grund for det system af beregningsprogrammer som overenskomstforhandlingerne for kommunerne og regionerne baserer sig på, og samtidig anvendes data både arbejdsgiverne KL og RLTN samt personaleorganisationerne, hvorved KRL dermed understøtter Den danske arbejdsmarkedsmodel.

KRL ledes af en bestyrelse med repræsentanter fra KL, Danske Regioner, Finansministeriet, Økonomi- og Indenrigsministeriet og Danmarks Statistik, og personaleorganisationerne er repræsenteret som observatører. KRL er finansieret af en grundbevilling på Finansloven.

KRL's bemærkninger til lovforslaget

I lyset af KRL's aktiviteter og formål, skal vi understrege vigtigheden af, at de muligheder for at fastsætte nationale bestemmelser, der følger af forordningen, og som det foreliggende lovforslag tager sigte på at udmønte, i nødvendigt omfang kommer til at understøtte KRL's virksomhed, så denne kan videreføres.

Vi er særligt opmærksomme på, at lovforslaget tilsyneladende ikke udnytter den hjemmel, der følger af forordningens artikel 89, stk. 2 til at fastsætte nationale undtagelser fra de rettigheder, der følger af artikel 15, 16, 18 og 21, når oplysningerne behandles til videnskabelige eller historiske forskningsformål eller til statistiske formål, hvoraf sidstnævnte må omfatte KRL. Vi vurderer, at en sådan undtagelse er central for KRL's muligheder for fortsat at kunne varetage sine opgaver. Vi skal derfor opfordre til, at en bestemmelse herom indarbejdes i lovforslaget.

KRL står naturligvis til rådighed for yderligere information og uddybende forklaring.

Med venlig hilsen

Erling Friis Poulsen
Formand for KRL's bestyrelse

Det Koordinerende Organ for Registerforskning

Justitsministeriet
Slotsholmsgade 10
1216 København K

Dato: 22. august 2017

KOR
Rigsarkivet
Rigsdagsgården 9
1218 København K

Telefon: 4171 7211
Mail: jkd@sa.dk
Web: registerforskning.dk

Sagsnr.: 16/09530

Det Koordinerende Organ for Registerforskning (KOR) takker for muligheden for at indgive høringssvar vedr. Udkast til forslag til databeskyttelsesloven.

KOR er overordnet set tilfredse med, at vilkårene for at bedrive registerforskning i Danmark forventeligt ikke bliver ændret med den nye lovgivning, hvorfor forskerne stadig vil kunne udnytte det tore potentiale, der er i at anvende de unikke, danske registre til gavn for sundhed, demokrati og samfundsøkonomi.

KOR støtter, at der ifølge § 10 stk 4. under visse omstændigheder kan gives mulighed for, at data, der er behandlet i forbindelse med sundhedsvidenskabelig forskning, senere kan behandles i andet end statistiks eller videnskabeligt øjemed, hvis det er nødvendigt for den registreredes vitale interesser. KOR mener, at dette understøtter muligheden for et samspil mellem forskning og samfundets ambitioner om individuel behandling af patienter i sundhedssystemet.

Venlig hilsen

Henrik Toft Sørensen
Professor, formand for KOR

København d. 22.08.2017

Høring over udkast til forslag til databeskyttelsesloven

Kreativitet & Kommunikation takker for muligheden for, at komme med høringssvar til Justitsministeriets forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Vi repræsenterer en branche, hvor data har meget stor betydning, idet markedsføring bl.a. gøres relevant, ved at modtageren er nærmere bestemt. Data er ligeledes et vigtigt redskab i den efterfølgende proces, da det hjælper til optimering – også for brugeroplevelsen og for videreudvikling. Data er generelt et vigtigt element i vores medlemmers daglige arbejde og forordningen og den nationale lov vil derfor få stor indflydelse for vores branche.

Videregivelse - § 13

Persondataforordningen indeholder ikke særlige regler om videregivelse af personoplysninger til brug for markedsføring og vi mener derfor, at det kan være problematisk, hvis man viderefører reglen fra persondataloven så udgangspunktet for videregivelse kræver et samtykke.

Med forordningen vil videregivelse kunne finde sted, hvor der er hjemmel til det i de almindelige behandlingsregler – med kravet om samtykke indskrænkes hjemmelsgrundlaget således betydeligt.

Vi mener at det er væsentligt at man ikke begrænser den erhvervsmæssige brug af data unødigt og strengere end forordningen lægger op til.

Åbningen for videregivelse uden samtykke i form af § 13, stk. 2 er begrænset til de situationer, hvor der er tale om generelle kundeoplysninger til inddeling i kundekategorier og hvor interesseafvejningsreglen hjemler det. Vi mener som udgangspunkt, at interesseafvejningen mellem erhvervsdrivende og de registrerede bør falde ud så behandling af personoplysninger til brug for direkte markedsførings som udgangspunkt er en berettiget interesse, hvilket også er sådan vi læser bemærkningerne.

Begrænsningen til alene at være generelle kundeoplysninger, mener vi dog er problematisk, hvis dette ikke følger direkte af forordningen. Følger det ikke af forordningen gøres hjemlen således om muligt endnu mere snæver for de erhvervsdrivende.

Vi er naturligvis bekymrede over, at man i den nationale lov øger forbrugerbeskyttelseshensynet, udover det der udspringer af forordningen. Hele omdrejningspunktet for forordningen har netop været dette beskyttelseshensyn og vi finder det derfor unødigt og uhensigtsmæssigt regulerende med en dansk "ekstra beskyttelse". Hvis vi har danske særregler på dette område, begrænser det også de danske erhvervsdrivendes konkurrenceevne på tværs af lande og medier.
Vi repræsenterer en række erhvervsdrivende, der behandler data på en måde, så markedsføringen optimeres, gøres relevant og konstant udvikler sig – med denne regel kan man potentielt skabe en begrænsning af dette arbejde, hvilket vi selvfølgelig ikke støtter. Danmark er kendt for høj forbrugerbeskyttelse, men vi mener man bør huske, at der er tale om en forordning, der har direkte virkning i landet og derfor er kilden til fortolkning.
Det er derfor vores opfordring, at man ikke ved fortolkning af interesseafvejningsreglen begrænser de erhvervsdrivende unødigt i forhold til forordningens hensigt og at man genovervejer hvorvidt § 13 er nødvendig som den er foreslået idet de registrerede allerede er beskyttet af de almindelige behandlingsregler.

Sanktioner overfor offentlige myndigheder - § 41, stk. 5

Da der ikke er taget stilling til spørgsmålet om sanktioner overfor offentlige myndigheder, er denne del af høringssvaret udtryk for vores holdning til brug for den endelige stillingtagen.
Vi mener helt principielt at de offentlige myndigheder skal straffes under samme forudsætninger som de private erhvervsdrivende – reglerne er lavet for at beskytte de registrerede, hvilket bør være uafhængigt af, hvor de er registreret. Der findes i vores optik ikke en legitim grund til at skelne, når man ser på data, behandling og mulig risiko. De offentlige myndigheder har ofte meget mere personfølsomt data, end det der findes hos de private erhvervsdrivende.
Som borger skal man kunne have tillid til de offentlige myndigheders behandling og opbevaring af oplysninger. I den optik er det klart, at de registrerede skal vide, at der selvfølgelig er konsekvenser, så der vil blive slået ned i tilfælde af lovovertrædelser – både hos private og hos myndigheder.
Når man kigger på Datatilsynets sager, omhandler de primært offentlige myndigheder. Dette er ikke et udtryk for, at de private nødvendigvis overholder reglerne til punkt og prikke, men nok nærmere et udtryk for ressourcer. Ikke desto mindre må det ses som et udtryk for, at der ikke er så godt styr på det hos de offentlige myndigheder som det kunne ønskes. Problemet er i den forbindelse, at en løftet pegefinger fra tilsynet næppe ændrer noget i praksis. Ændringer koster tid og penge og hvis der ingen konsekvenser er forbundet med ikke at ændre, så er det svært at forestille sig, hvorfor man skulle gøre det. Derfor bør der fra 25. maj 2018, være mere end blot en løftet pegefinger.
De private erhvervsdrivende vil blive tvunget til, at leve op til forordningen, fordi bødestørrelserne er af en

kaliber som præventivt vil virke afskrækkende og potentielt kan lukke virksomheder. Men den præventive effekt over for de offentlige myndigheder vil være ikke eksisterende, hvis ikke sanktionerne er gældende for dem.
Vi er samtidig bevidste om, at der med denne holdning følger en politisk diskussion af hvorfra en bøde til en offentlig myndighed skal betales og at der rent økonomipolitisk kan være en praktisk udfordring i at det reelt i sidste ende kan have en konsekvens for de registrerede og dermed give bagslag. Vi mener man bør kunne finde en løsning på denne problematik, som det kendes fra andre retsområder, hvor der pålægges bøder.

Administrativt bødeforlæg - § 42

Vi mener som udgangspunkt, at man skal være påpasselig med at give kompetence til at udstede administrative bødeforlæg, idet det kan have betydning for retssikkerheden. Det er vigtigt, at bøder udstedes på et objektivt grundlag, hvilket i vores optik kræver, at der er et fast fundament for at give en administrativ kompetence. Det er derfor vores opfattelse, at man ikke på nuværende tidspunkt bør indføre en kompetence for administrative bødeforlæg, men at man bør afvente en fast praksis som kan være grundlag for kompetencen. En sådan praksis ses fx på spamområdet (Markedsføringsloven), hvor der er en fast praksis for prisen på overtrædelse af bestemmelsen – her mener vi, som udtrykt i høringssvar på området, at det giver god mening, at give kompetencen til Forbrugerombudsmanden i ikke kontroversielle sager under en vis grænse.
Derfor er vi ikke afvisende for, at man på sigt kan overlade kompetencen til Datatilsynet, men vi mener ikke at § 42 på nuværende tidspunkt har en eksistensberettigelse.

Vi stiller os gerne til rådighed for uddybninger eller spørgsmål i forbindelse med høringssvaret.

Med venlig hilsen

Cecilie Kunz Paulsen
Juridisk rådgiver, Kreativitet & Kommunikation

ckp@kreakom.dk
+45 41 31 60 08

KRIMINAL FORSORGEN

Pinerluttunik Isumaginnittoqarfik

HOVEDKONTORET

Justitsministeriet

Databeskyttelseskontoret

Nuuk, den 15. august 2017

Ref.: MW

Vedrørende høring over udkast til forslag til databeskyttelsesloven

Kriminalforsorgen i Grønland har den 14. juli 2017 modtaget Justitsministeriets høring over udkast til forslag til databeskyttelsesloven. Kriminalforsorgen i Grønland har ingen bemærkninger hertil.

Med venlig hilsen

Naaja H. Nathanielsen

Direktør

Aqqusinersuaq 4, Postboks 369
3900 Nuuk

Telefon: (00 299) 34 75 00
Telefax: (00 299) 34 82 15

Mail: kf@kriminalforsorgen.gl
Hjemmeside: www.kriminalforsorgen.gl

Kræftens Bekæmpelse

21. august 2017

Justitsministeriet
Lovafdelingen, Databeskyttelseskontoret
Slotholmsgade 10
1216 København K

Sendt til: databeskyttelse@jm.dk og jm@jm.dk

Direktionen

Strandboulevarden 49
2100 København Ø
Tlf +45 3525 7500
www.cancer.dk

UNDER PROTEKTION AF
HENDES MAJESTÆT DRONNINGEN

Sagsnr. 2016-7910-0008 Høring over udkast til forslag til databeskyttelsesloven

Ved e-mail af 7. juli 2017 har Justitsministeriet sendt ovennævnte udkast til høring hos en lang række interessenter, herunder Kræftens Bekæmpelse.

Kræftens Bekæmpelse glæder sig over, at det med persondataforordningen samt forslaget til supplerende bestemmelser til persondataforordningen fortsat vil være muligt at gennemføre registerbaseret folkesundheds- og sundhedsvidenskabelig forskning på det høje niveau, som Danmark er internationalt anerkendt for.

I bemærkningerne til lovforslaget forudsættes det, at *der ikke sker nogen indskrænkning i forhold til de muligheder, som dataansvarlige har for at foretage undersøgelser i statistisk eller videnskabeligt øjemed efter den gældende persondatalov (s. 270),* hvilket indebærer, at det fortsat være muligt at:

- indsamle personhenførbare helbredsoplysninger i befolkningsregistre, såsom Cancerregisteret, og at sikre høj datakvalitet i befolkningsregistre gennem komplet dækning af populationen samt brug af cpr-numre i registreringen.

- anvende registerdata til folkesundheds- og sundhedsvidenskabelige forskningsformål uden samtykke samt at koble data fra forskellige befolkningsregistre på baggrund af cpr-numre til disse forskningsformål (jf. forslagets §11, Stk.2, nr.3).

Kræftens Bekæmpelse finder det videre særdeles positivt, at

- indsigtsretten, jf. forslagets §22, Stk. 5, (som i gældende ret) ikke vil finde anvendelse, hvis oplysningerne alene behandles i videnskabeligt øjemed eller i det tidsrum, som kræves for at udarbejde statistikker. Indsigtsretten bør løftes af den registeransvarlige, idet den vil være uforholdsmæssig vanskelig at løfte for den enkelte forsker.

- der med forslagets §10, Stk. 4 gives mulighed for fastsatte regler om, at oplysninger behandlet til sundhedsvidenskabelige forskningsformål senere vil kunne behandles i

andet øjemed, hvis dette er nødvendigt af hensyn til varetagelse af den registreredes vitale interesser.

Det er imidlertid afgørende, at bestemmelsen er tiltænkt et meget snævert anvendelsesområde, og at der ved fastsættelsen af de nærmere regler for dette, indføres betingelser, som beskrevet på s. 271-272 i bemærkningerne i lovforslaget. Det vil sige betingelse om samtykke fra den registrerede eller vurdering ved sagkyndig komité til sikring af individbeskyttelse, selvbestemmelse og retten til ikke at vide, samt at videregivelsen af de omhandlede oplysninger til den registrerede sker via den patientansvarlige læge.

Kræftens Bekæmpelse bemærker imidlertid, at

- Lovforslagets §2, Stk. 5 lægger op til, at bestemmelserne alene finder anvendelse på oplysninger om en afdød i 10 år efter vedkommendes død.

  Kræftens Bekæmpelse undrer sig over, at Datatilsynets praksis med at omfatte afdøde personers helbredsoplysninger af Persondataloven ikke videreføres med de supplerende bestemmelser til Databeskyttelsesforordningen.

  Oplysninger om helbredsforhold udgør en særlig kategori af oplysninger, jf. forordningen, og patienter og pårørende oplever i høj grad, at oplysninger om helbredsforhold er blandt de mest private og følsomme oplysninger.

  Kræftens Bekæmpelse er bekymret for, at det kan få negativ betydning for fortroligheden mellem læge og patient, hvis oplysninger om helbred og i øvrigt rent private forhold falder uden for loven om databeskyttelse efter blot 10 år.

  Videre bidrager udviklingen inden for sundhedsvidenskaben til, at oplysninger om den enkeltes helbred i stigende grad rummer information om biologiske slægtninges helbred eller mulige helbredstilstand. Dette kan potentielt være stigmatiserende.

  Hensynet til afdøde og dennes pårørende rækker således videre end det hensyn til afdødes eftermæle, som der henvises til i bemærkningerne til lovforslaget (s. 161).

  Kræftens Bekæmpelse opfordrer til, at gældende praksis videreføres, evt. under lovforslagets §2, Stk. 6, eller at der udarbejdes en særlig bestemmelse herfor for sundhedsdata

- Med lovforslaget lægges der op til, at anmeldepligten ved Datatilsynet bortfalder for registerbaseret forskning.

  Kræftens Bekæmpelse finder det yderst vigtigt at sikre størst mulig transparens om behandling af danskernes helbredsoplysninger til forskningsformål og bemærker, at transparens omkring databehandling også er en af intentionerne med Databeskyttelsesforordningen.

Lovforslaget lægger op til, at forskningen også fremover skal finde sted i henhold til gældende etik, databeskyttelses- og sundhedslovgivning, men uden myndighedsgodkendelse.

Kræftens Bekæmpelse finder det ærgerligt, at anmeldepligten bortfalder for så vidt, at den ikke erstattes med yderligere tiltag end fortegnelseskravet til den enkelte dataansvarlige, der i henhold til artikel 9 vil gælde alle sundhedsdata. Disse fortegnelser er ikke offentlige, men stilles til rådighed for tilsynsmyndigheden på forlangende. Herved mistes et nationalt overblik over brugen af bl.a. sundhedsdata og transparens for borgerne om, hvad data bruges til. Samtidig mistes en nøgle til inspektion fra tilsynsmyndigheden, som især vil være bekymrende, når det drejer sig om små organisationer/databehandlere, der ikke har persondata, og disses beskyttelse som en integreret og naturlig del af deres virke.

Kræftens Bekæmpelse finder det centralt, at nye bestemmelser på området bidrager til en forenkling af reglerne omkring behandling af helbredsoplysninger til forskning- og statistiske formål med henblik på at skabe størst mulig åbenhed og sikkerhed for danskerne omkring behandlingen af sundhedsdata.

Med henblik på at sikre størst mulig åbenhed, regelenkelthed samt overholdelse af gældende videnskabsetik opfordrer Kræftens Bekæmpelse til, at der etableres en simpel national fortegnelse, hvor den dataansvarlige er forpligtet til at anføre formål med behandlingen og hvilke persondata der behandles. Alternativt, at der indarbejdes bestemmelser i Komitéloven om videnskabsetisk vurdering af de forskningsprojekter, som på nuværende tidspunkt blot er anmeldepligtige, evt. efter svensk forbillede.

En ensartet videnskabsetisk vurdering og godkendelse af de enkelte forskningsprojekter vil udgøre en databeskyttelsesgaranti for den registrerede, som samtidig kan bidrage til at opretholde tilliden blandt befolkning til forskningen. Samtidig bliver det klarere, at data ikke flyder og udleveres helt frit.

Yderligere bemærkninger:

- Risiko for vilkårlighed omkring myndighedsbesøg, hvis der ikke er en samlet fortegnelse over forskningsaktiviteter. Hvor skal Datatilsynet lede?
- Hvordan sikres det, at procedurer omkring dataadgang og -udlevering til forskningsformål fortsat er smidige og ensartede, når der ikke foreligger en myndighedsgodkendelse?

Med venlig hilsen

Leif Vestergaard Pedersen
Adm. direktør

KØBENHAVNS UNIVERSITET

Til:
Justitsministeriet, databeskyttelseskontoret

SAGSNOTAT

22. AUGUST 2017

Vedr. Høring af forslag til databeskyttelseslov

Sagsbehandler Klaus Kvorning Hansen

KONCERN-IT

MOB 29354204

klkh@adm.ku.dk

REF: KLKH

Justitsministeriet har anmodet om bemærkninger til udkast til forslag til databeskyttelseslov, som skal supplere anvendelsen af reglerne i databeskyttelsesforordningen i Danmark.

Københavns Universitet har følgende bemærkninger:

Til § 4, stk. 1,

Det kan overvejes at tilføje, at loven gælder uanset om den registreredes nationalitet og opholdssted er inden for EU eller i et tredjeland. Det fremgår af de specielle bemærkninger til § 4, stk. 1, at forslaget har til hensigt at videreføre gældende ret i persondatalovens § 4. Det fremgår af "Lov om behandling af personoplysninger med kommentarer af Kristian Korfits Nielsen og Henrik Waaben", at loven gælder, hvis den dataansvarlige er etableret i Danmark og det er uden betydning, hvilken nationalitet den registrerede har og hvor den pågældende befinder sig.
I forskningsprojekter, hvori der indgår behandling i Danmark af personoplysninger indsamlet i tredjelande, har det givet anledning til tvivl om loven finder anvendelse. En præcisering er derfor ønskelig.

Til § 5.

Bestemmelsen indeholder en bestemmelse svarende til forordningens artikel 6, stk. 4 samt en bemyndigelse til at fastsætte regler, som giver offentlige myndigheder hjemmel til at viderebehandle oplysninger til andre formål end oplysningerne var indsamlet til. Bestemmelsen har sammenhæng med forordningens artikel 5, hvorefter det er lovligt at viderebehandle

oplysninger til bl.a. videnskabelige eller historiske forskningsformål. Det er uklart, om artikel 5, stk. 1, litra b), giver hjemmel til at anvende oplysninger indsamlet til et konkret forskningsprojekt i et senere forskningsprojekt inden for samme forskningsområde eller et helt andet forskningsområde. Såfremt artikel 5, stk. 1, litra b) ikke giver hjemmel til at genanvende forskningsdata i senere forskningsprojekter, kan det overvejes at lade bemyndigelsen i § 5, stk. 2 omfatte genanvendelse af forskningsdata generelt eller i et givent omfang.

Til § 10.

Det er afgørende for den danske registerforskning, at såvel almindelige personoplysninger efter forordningens artikel 6 og følsomme personoplysninger efter forordningens artikel 9 kan indhentes og behandles til forskningsformål uden forudgående indhentelse af den registreredes samtykke. Forordningens artikel 9, stk. 2, litra j) åbner mulighed for registerforskning i følsomme oplysninger uden forudgående indhentelse af samtykke. En tilsvarende bestemmelse findes ikke i § 6 for så vidt angår almindelige personoplysninger. Det kan med fordel præciseres i lovens § 10, at registerforskning uden den registreredes forudgående samtykke er mulig både for så vidt angår almindelige og følsomme personoplysninger. De gældende udtalelser fra Datatilsynet i forbindelse med universiteternes fællesanmeldelser tillader videregivelse af oplysninger til brug for andre undersøgelser i statistik eller videnskabeligt øjemed, der foretages for dataansvarlige etableret i Danmark. Det foreslås, at en tilladelse til videregivelse til andre undersøgelser i statistisk eller videnskabeligt øjemed fastsættes direkte i loven suppleret af betingelser svarende til de gældende betingelser i Datatilsynets udtalelser. Betingelserne kan evt. fastsættes på bekendtgørelsesniveau.

Til § 11.

Det fremgår af forslaget, at offentlige myndigheder alene må anvende personnumre som journalnumre, og at private må anvende personnumre til videnskabelige eller statistiske formål. Da universiteterne udfører forskning i offentligt regi, bør det også være muligt for universiteterne at anvende personnumre til videnskabelige formål, når det ikke er muligt at anvende pseudoanonymiserede eller anonymiserede oplysninger.
Selv om kravene til samtykkets udtrykkelighed er skærpet i forordningens artikel 7, findes det betænkeligt, at det skal være muligt at give samtykke til offentliggørelse af personnumre, især hvis dette samtykke indgår i et generelt samtykke fx til deltagelse i et forskningsprojekt.

Til § 29

Det fremgår af bestemmelsens stk. 2, at: ”Datatilsynets medlemmer og personale har mod behørig legitimation til enhver tid uden retskendelse adgang til alle lokaler, hvorfra en behandling af personoplysninger foretages.” Mange forskere har samarbejder med andre forskere, som er ansat på udenlandske universiteter. Disse får adgang til data på Danmarks Statistik under Forskerordningen. Adgangen sker ved, at de pågældende forskere logger på en server, som fysisk befinder sig i Danmark, dvs. på Københavns Universitet, gennem en VPN forbindelse, og derigennem logger på Danmarks Statistiks servere. Disse forskere befinder sig således ikke fysisk i Danmark, men de servere, hvorpå data ligger, befinder sig på Danmarks Statistik. Det er afgørende, for at sådanne internationale samarbejder kan eksistere, at § 29, stk. 2 fortolkes således, at Datatilsynet skal have adgang til de lokaler, hvor data-serverne befinder sig, dvs. Danmarks Statistik, og ikke de lokaler hvor forskerne faktisk sidder, når de arbejder på data.

Til § 41

Lovforslaget, jf. § 41, stk. 5, undlader at stille forslag om sanktioner for offentlige myndigheder, der overtræder forordningen (og loven). Det formodes overladt til behandlingen i Folketinget. Det anbefales, at sanktioner over for offentlige myndigheder, hvor der ikke er handlet groft uagtsomt, begrænset til et minimum eventuelt i form af advarsler.

Generelt

Afslutningsvis skal bemærkes, at der må påregnes mærkbare meromkostninger i forbindelse med universitetets overholdelse af forordningen f.eks. til privacy assesment analysis og til ansættelse af en databeskyttelsesrådgiver. Disse omkostninger bør KU kompenseres for via bevillinger over de årlige finanslove.

Lægeforeningen

Formanden

22. august 2017
Jr. 2017-5810

Domus Medica
Kristianiagade 12
2100 København Ø

Tlf.: 3544 8500
E-post: dadl@dadl.dk

www.laeger.dk

Høringssvar

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

Patienter skal trygt kunne henvende sig til sundhedsvæsenet i tillid til, at deres sundhedsdata anvendes efter klare retningslinjer

Lægeforeningen mener, at den foreslåede nye bemyndigelsesbestemmelse i lovudkastets § 5, stk. 3 er for vidtgående.

Bestemmelsen gør det muligt for en minister, efter forhandling med justitsministeren, at fastsætte regler om, at offentlige myndigheder må viderebehandle personoplysninger til andre formål, end de var indsamlet til.

Bemyndigelsesbestemmelsen kan anvendes til i bekendtgørelsesform at fastsætte regler om videregivelse af oplysninger fra én myndighed til en anden myndighed.

Det er Lægeforeningens opfattelse, at der er tale om en meget vidtgående bemyndigelsesbestemmelse, der bryder med den hidtidige persondatalov og, efter vores opfattelse, ikke synes at være i databeskyttelsesforordningens ånd.

Forordningen bestemmer i artikel 23, at medlemslandene i Den europæiske Union har et rum for national selvbestemmelse, hvorefter der i stk. 1, pkt. a-j oplistes en række områder og hensyn, der kan begrunde nationale særregler. Ingen af de nævnte hensyn synes at kunne begrunde nødvendigheden af en generel bemyndigelsesbestemmelse som den foreslåede i lovforslagets § 5, stk. 3.

Retspolitisk er den foreslåede bemyndigelsesbestemmelse i § 5, stk. 3 betænkelig, da integritetsbeskyttelsen udvandes, ligesom det synes dårligt overensstemmende med det persondataretlige finalité-princip om formålsbestemthed.

Endelig er det juridisk uheldigt, at der under en fremtidig retstilstand, hvor databeskyttelsesloven skal gælde parallelt med forordningen, vil være en tvivlsom overensstemmelse mellem forordningen principper og den nationale særlovgivning.

Netop på sundhedsområdet skræmmer sporene, idet der er eksempler på indsamling af data til ét formål, som efterfølgende anvendes til andre formål, der ikke kunne forudses ved den oprindelige indsamling.

Det forekommer unødvendigt og utryghedsskabende, at der med lovforslaget lægges op til, at de enkelte ressortministre efter forhandling med justitsministeren kan fastsætte regler, der indebærer, at personoplysninger anvendes ud over det formål, som de oprindelig var indsamlet til. Der er ingen grund til, at en sådan anvendelse ikke skulle kunne ske ved lovgivning i stedet. Derved sikres parlamentarisk kontrol, ligesom de relevante høringsberettigede parter kan give deres besyv med – til gavn for den demokratiske proces.

Ønsket om en bred politisk inddragelse ved brug af sundhedsdata følger også af den politiske aftale, som blev indgået i februar 2017 om "Bedre sundhed gennem moderne og sikker brug af data". Aftalen indeholder syv principper for udvikling og brugen af sundhedsdata. Én af principperne omhandler "Moderne og tryg lovgivningsramme". Det fremgår, at

"Det skal sikres, at Folketinget løbende kan diskutere og vedtage lovændringer, der sikrer, at den gældende lovgivning løbende tilpasses udviklingen, herunder nye undersøgelses- og behandlingsmetoder samt de teknologiske muligheder for betryggende udveksling af data, og at lovgivningen balancerer væsentlige etiske principper om bl.a. fortrolighed, beskyttelse af individet gennem fx. Samtykke og myndighedsgodkendelser, solidaritet og tillid".

Behandling af oplysninger i statistisk eller videnskabeligt øjemed
Lægeforeningen støtter lovforslaget om at videreføre de samme bestemmelser fra den nuværende persondatalovs § 10 om behandling af oplysninger i statistisk eller videnskabeligt øjemed, jf. dog særlige bemærkninger til den nye bemyndigelsesbestemmelse i lovforslaget § 10, stk. 4 nedenfor.

Det fremgår således af den foreslåede bestemmelse i § 10, stk. 1, at f.eks. de følsomme oplysninger nævnt i forordningens artikel 9 må behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig af hensyn til udførelsen af undersøgelserne. Bestemmelsen kræver således ikke samtykke.

Lægeforeningen mener dog, at der med fordel kunne etableres og kommunikere en tydeligere beskrivelse af, hvordan "væsentlig samfundsmæssig betydning" skal fortolkes. Det vil være et godt skridt i retningen af at skabe større gennemsigtighed omkring forskningsanvendelsen af helbredsmæssige oplysninger/sundhedsdata.

Den foreslåede bestemmelse i § 10, stk. 2 svarer til den nuværende persondatalov og indebærer, at personoplysninger herunder helbredsoplysninger,

som er behandlet f.eks. i forbindelse med et forskningsprojekt efter bestemmelsen i § 10, stk. 1 ikke senere må behandles i andet end videnskabeligt eller statistisk øjemed. Lægeforeningen bemærker, at Datatilsynet har udtalt, at bestemmelsen i § 10, stk. 2 ikke kan suppleres med samtykkebestemmelserne i den nuværende persondatalov.

Lægeforeningen er opmærksom på, at hverken de nuværende regler i persondatalovens § 10, stk. 2 eller den foreslåede § 10, stk. 2 gør det muligt, at videregive personoplysninger herunder helbredsoplysninger, der stammer fra forskningssammenhænge til patientbehandling af den specifikke person, som oplysningerne vedrører.

Der foreslås derfor en ny bemyndigelsesbestemmelse til sundhedsministeren i lovforslagets § 10, stk. 4, som gør det muligt, efter forhandling med justitsministeren, at fastsætte regler om, at oplysninger omfattet af forordningens artikel 6 og 9, som er behandlet med henblik på at udføres sundhedsvidenskabelig forskning og statistik senere kan anvendes til andre formål end videnskabelige eller statistiske formål, hvis en sådan behandling er nødvendig til varetagelse af den registreredes vitale interesser.

Lægeforeningen er enig i, at adgangen til at behandle herunder at videregive personoplysninger fra forskningssammenhæng til andre formål end forskning og statistik bør begrænses til helt særlige situationer og alene til de situationer, som er nævnt i bemærkningerne til lovforslaget dvs. i forbindelse med sekundære fund og ved beslutningsstøtte ved valg af behandling (personlig medicin).

Lægeforeningen anerkender, at der i disse særlige situationer kan være behov for en klar hjemmel til at behandle herunder at videregive oplysninger, når der er i forbindelse med et forskningsprojekt er fremkommet oplysninger om, at den registrerede lider af livstruende eller klart alvorlig sygdom, som enten kan behandles, forebygges eller lindres, og at det derfor er nødvendigt af hensyn til personens vitale interesser at behandle herunder videregive oplysningerne med henblik på at informere den person, som det omhandler om dette fund og dels til at benytte oplysningerne til at vurdere om og i givet fald hvilken patientbehandling, som bør iværksættes.

Lægeforeningen støtter endvidere, at det kun er sundhedspersoner omfattet af tavshedspligten i sundhedslovens § 40, der kan videregive oplysninger om livstruende eller klart alvorlige sygdomme til den registrerede.

Behov for tydeliggørelse af bemyndigelsesbestemmelsen
Lægeforeningen mener, at beskyttelse af individets følsomme herunder helbredsmæssige oplysninger og beskyttelsen af tilliden til anvendelsen af disse oplysninger i sundhedsvidenskabelig og sundhedsstatistisk sammenhæng er vigtigt.

Lægeforeningen er derfor opmærksom på vigtigheden af, at den nye bemyndigelsesbestemmelse i lovforslagets § 10, stk. 4 fremstår tydelig. Det er vores opfattelse, at bemærkningerne til lovforslaget herunder rækkevidden af forslaget på enkelte punkter bør tydeliggøres.

Af bemærkningerne fremgår det, at det senere kan komme på tale, at fastsætte bestemmelser om, at oplysninger, der stammer fra sundhedsvidenskabelige statistiske undersøgelser, ligeledes vil kunne behandles med henblik på varetagelse af den registreredes vitale interesser, fx. statistik, der bruges til patientsikkerhedsformål, monitorering mv. Bemærkningen kan med fordel uddybes herunder med konkret eksempler.

Af lovforslagets bemærkninger (s. 192) fremgår det, at der skal gives mulighed for en videre behandling til andre formål end videnskabelige eller historiske forskningsformål på baggrund af samtykke fra den registrerede eller ved særlige omstændigheder, **herunder** (Lægeforeningens fremhævelse) hensynet til den registreredes (vitale) interesser.

Lægeforeningen finder ikke, at der er overensstemmelse mellem den konkrete bemærkning i lovforslagets § 10, stk. 4s ordlyd. Af § 10, stk. 4 fremgår det, at en videre behandling skal "være nødvendig af hensyn til varetagelse af den registreredes vitale interesser". Lægeforeningen forudsætter, at opfyldelse af kravet om "hensyn til varetagelse af den registreredes vitale interesser" altid skal være til stede – også i situationer, hvor der forud ønskes indhentet et samtykke fra den registrerede, som nævnt i et eksempel i bemærkningerne (s. 272). Dette bør præciseres.

Lægeforeningen ønsker med andre ord at understrege, at den foreslåede § 10, stk. 4 alene kan accepteres så længe begrebet "patientens vitale interesser" fortolkes restriktivt, som henvisende til den enkelte patients vitale interesse i én konkret situation. Hvis det foreslåede § 10, stk. 4 anvendes til at muliggøre en bredere genanvendelse af oplysninger til andre formål end forskning og statistik, risikerer det at underminere accepten af, at personoplysninger kan anvendes til forskning og statistik, hvilket ville være meget problematisk.

I bemærkninger til bestemmelsen beskrives forskellige situationer, hvor det er hensigten af udmønte bemyndigelsen. Det fremgår således, at der i forbindelse med behandling herunder videregivelse af fund i forbindelse med sundhedsvidenskabelige forskningsprojekter og sundhedsvidenskabelige statistiske undersøgelser vil blive stillet krav om, at der skal foreligge et samtykke fra den registrerede (afgivet inden forskningsprojektet) eller på anden vis være passende foranstaltninger, der sikrer den registreredes interesser og understøtter individbeskyttelse og selvbestemmelse, herunder retten til ikke at vide (f.eks. høring af sagkyndig komité).

Lægeforeningen savner, at bemærkningerne beskriver, hvilke "passende foranstaltninger", der kan være tale om, og at bemærkningerne uddyber bemærkningen om sagkyndig komité.

Manglende sanktioner for offentlige myndigheder
Vedrørende strafbestemmelser bemærker Lægeforeningen, at lovforslaget er tavst på dette punkt. Det fremgår af lovforslagets § 41, stk. 5, at sanktionsspørgsmålet i forhold til offentlige myndigheder udestår.

Med henblik på det videre lovgivningsarbejde gør Lægeforeningen opmærksom på, at det ud fra almindelige lighedsbetragtninger vil virke stødende, hvis ikke private og offentlige dataansvarlige er ligestillede.

Netop på sundhedsområdet er der i det nære sundhedsvæsen store grupper af private aktører, og det vil fremstå helt arbitrært, hvis eksempelvis en alment praktiserende læges forsømmelse skulle takseres anderledes end en regionskliniks. Tilsvarende kan anføres om forholdet mellem praktiserende speciallæger og eksempelvis sygehusambulatorier.

Med venlig hilsen

Andreas Rudkjøbing
Formand for Lægeforeningen

Lægemiddel
Industri
Foreningen

Lersø Parkallé 101
2100 København Ø
Telefon 39 27 60 60
Telefax 39 27 60 70

info@lif.dk
www.lif.dk

Justitsministeriet
Lovafdelingen
Slotsholmsgade 10
1216 København K

Sendt per e-mail til databeskyttelseskontoret@jm.dk

22. august 2017

Vedrørende høring over udkast til forslag til databeskyttelsesloven (sagsnr. 2016-7910-0021)

Lif ønsker indledningsvist at takke for muligheden for at komme med bemærkninger til det fremsendte udkast til forslag til databeskyttelsesloven.

Det er af afgørende betydning for lægemiddelindustrien – og for sundhedsområdet i bred forstand – at implementeringen og den praktiske administration af Databeskyttelsesforordningen (2016/679), der træder i kraft den 25. maj 2018, understøtter, at der fortsat kan gennemføres effektiv og værdifuld forskning af høj kvalitet i Danmark. Forskning med afsæt i danske sundhedsdata er bl.a. fundament for udvikling af nye lægemidler og nye behandlinger, der kommer både patienter og samfundet til gavn. Anvendelse af sundhedsdata er hjørnestenen i den forskning, der skal bidrage til udvikling af personlig medicin, og som vil sikre, at lægemidlers udvikling og anvendelse målrettes den enkelte patient. Danmark har gode forudsætninger for at være helt i front i forhold til udvikling af personlig medicin, og det har også været medvirkende årsag til, at regeringen og Danske Regioner har udarbejdet og igangsat en national strategi for Personlig Medicin (2017-2020) – en national strategi, der nyder bred politisk opbakning, og som involverer både offentlige og private forskere, universiteter, hospitaler og patientorganisationer m.fl.

Databeskyttelsesforordningen og databeskyttelsesloven udgør en central ramme for dansk sundhedsregisterforskning, klinisk lægemiddelforskning og den forskning, der skal laves i regi af den nationale strategi for personlig medicin. Derfor er det også vigtigt, at den nye databeskyttelseslov, der supplerer og gennemfører databeskyttelsesforordningen, skaber en utvetydig ramme, som sikrer, at dansk forskning fortsat kan stå stærkt.

For så vidt angår reglerne omkring behandling af oplysninger i statistisk eller videnskabeligt øjemed - lovforslagets § 10 viderefører persondatalovens § 10 - deler Lif ministeriets opfattelse af, at den nuværende persondatalovs § 10 skaber en fornuftig balance mellem hensynet til forskning og statistik og hensynet til beskyttelsen af personoplysninger. Efter lovforslagets § 10, stk. 1 vil der kunne behandles oplysninger som nævnt i databeskyttelsesforordningens artikel 9, stk. 1, og artikel 10, såfremt behandlingen alene finder sted med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig af hensyn til udførelsen af undersøgelserne. I bemærkningerne forudsættes det, at der ikke sker nogen indskrænkning i forhold til de muligheder, som dataansvarlige har for at foretage undersøgelser i statistisk eller videnskabeligt øjemed efter den gældende persondatalov. Denne forudsætning er vigtig, da vi også noterer os, at ordlyden af lovforslagets § 10, stk. 1 er mere restriktiv end krævet af databeskyttelsesforordningen, jf. artikel 9, stk. 2, litra j:

"Behandling er nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser."

Med henvisning til databeskyttelsesforordningens artikel 5, stk. 1, litra b skal Lif henstille til, at det præciseres i databeskyttelseslovens § 5, stk. 2, at viderebehandling af data ikke er uforenelig med databeskyttelseslovens § 5, stk. 1, når viderebehandlingen alene finder sted med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning.

Databeskyttelsesforordningens artikel 5, stk. 1, litra b:
"Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)."

Adgang til at forske videre på allerede indsamlede data, fx indsamlet ved kliniske studier eller i registre, fra en ny forskningsmæssig vinkel og med et nyt formål, er af stor videnskabelig betydning, idet det dels kræver mange ressourcer at indsamle data, og dels er det ikke i alle tilfælde muligt ud fra etiske regelsæt (jf. fx Lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter § 18) at indsamle samme type data to gange. Adgang til viderebehandling er vigtig, fordi nye forskningsteorier derved kan blive efterprøvet på eksisterende data.

Det ville være ønskeligt, hvis denne mulighed for at forske videre med nye formål på allerede eksisterende data kunne fremgå tydeligt af databeskyttelseslovens § 5, stk. 2, da dette dels vil være til stor gavn for den kliniske forskning og dels for forskningen i de danske sundhedsregistre og ikke mindst gavne Danmark i et internationalt perspektiv, hvor det vil være attraktivt at lægge sundhedsforskningsaktiviteter i Danmark.

Endelig finder Lif det vigtigt, at den danske gennemførelse af databeskyttelsesforordningen nøje overvåges og sammenholdes med tiltag og erfaringer fra de øvrige EU-medlemslande. Skal dansk lægemiddelforskning og sundhedsforskning fortsat være af høj international kvalitet og til gavn for både patienter og samfund, er det afgørende, at der ikke implementeres nationale bestemmelser eller udvikles nationale særpraksisser, der gør det sværere eller mindre attraktivt at gennemføre forskning i Danmark – forskning som omfatter behandling af personoplysninger.

Forskning med udgangspunkt i sundhedsdata er i dag en dansk styrkeposition, som skaber værdi for patienter og samfund, og som vi derfor skal værne om. Reguleringen af persondata står i den forbindelse helt centralt, da den dels udstikker de praktiske rammer for forskernes arbejde, og dels sikrer befolkningens tillid til forskningen. Begge dele er vigtigt, og den hidtidige praksis på området har understøttet dette. Vi vil derfor gerne fra Lifs side understrege vores opbakning til lovforslagets forudsætning om, at den nuværende praksis og de nuværende muligheder for at gennemføre forskning i Danmark ikke forringes.

Såfremt ovenstående giver anledning til spørgsmål eller ønske om uddybende dialog, står Lif naturligvis til rådighed herfor.

Med venlig hilsen

Jakob Bjerg Larsen
Chefkonsulent

Databeskyttelseskontoret 24. juli 2017
Justitsministeriet
databeskyttelseskontoret@jm.dk

Høringssvar over udkast til forslag til databeskyttelsesloven

Det er et stort problem for den kliniske forskning i Danmark at pseudonymiserede kliniske data, dvs. data hvor al personhenførbar information er fjernet og erstattet med en kode, ikke er undtaget fra loven. I forordningen (nr. 2016/679 af 27. april 2016) er pseudonymisering en forudsætning for at databehandling af kliniske data til forskningbrug overhovedet kan finde sted.

I USA er pseudonymiserede data udtrykkeligt undtaget fra databeskyttelses-lovgivning, og det har medført at National Institute of Health har kunnet oprette databaser hvor forskere deler deres pseudonymiserede data fra kliniske studier, der så kan genbruges i mange forskningprojekter.

Det er ikke muligt i Danmark, hvor dette ville betragtes som en overtrædelse af loven. Kliniske data kan altså ikke genbruges, og det fører til at kliniske forsøg må gentages i stedet for at genbruges. Det er ikke i de deltagende patienters interesse. Men også forskning der opfylder betingelserne i loven, sinkes i måneder eller år idet der kræves omfattende og komplicerede databehandleraftaler selv for pseudonyme data.

Uden den amerikanske undtagelse ville vores virksomhed ikke kunne havet udvikle sin cancerdiagnostik med amerikanske kliniske data. Omvendt mødes kliniske studier i Danmark, der søges internationalt publiceret, ofte netop med et krav om offentliggørelse af pseudonymiserede data, og det er ikke tilladt under forordningen.

Jeg henvendte mig omkring netop denne problemstilling til Kommisionen før forordningens vedtagelse, men fik at vide at min henvendelse ikke ville blive besvaret.

Tilbage står en mulighed for at Dansk lov præciserer, eller der fastsættes regler for, at pseudonyme data er undtaget fra loven, mens koden der tillader at knytte pseudonyme data til fysiske personer er omfattet af loven. Dette ville ikke på nogen made svække beskyttelsen af patienters kliniske data, men ville bringe Danmark på lige fod med USA i effektiv og hurtig klinisk forskning som skal føre til forbedret behandling og de produkter der skal sikre Danmarks fremtidige velstand.

Steen Knudsen, PhD
Forskningsdirektør
Medical Prognosis Institute A/S
steen@medical-prognosis.com

MODERNISERINGSSTYRELSEN

Notat

22. august 2017
MAHER/HCH/
LVM

Notat om høring over udkast til forslag til databeskyttelsesloven

Justitsministeriet (JM) har sendt udkast til forslag til databeskyttelsesloven i høring den 7. juli 2017.

Databeskyttelsesloven skal træde i kraft den 25. maj 2018, og vil eksistere sideløbende med databeskyttelsesforordningen. Databeskyttelsesloven vil supplere forordningen med nationale bestemmelser.

Moderniseringsstyrelsens konkrete bidrag til høringssvar er beskrevet nedenfor, og vedrører i overskriftsniveau følgende områder:

a) Udspecificering af status for CPR-numre
b) Indsigtsret i forbindelse med statistiske undersøgelser
c) Præcisering af regel om høring af Datatilsynet ved udarbejdelse af generelle retsforskrifter

A. Udspecificering af status for CPR-numre, jf. § 11
Lovens § 11, stk. 1, giver hjemmel til, at offentlige myndigheder kan behandle oplysninger om personnumre med henblik på en entydig identifikation eller som journalnummer.

CPR-numre er ifølge bemærkningerne til databeskyttelsesloven en almindelig personoplysning, og dermed ikke kræver ekstra sikkerhedsforanstaltninger. Det fremgår dog ikke specifikt af udkastet til loven, hvilken status CPR-nummeret har sikkerhedsmæssigt, jf. artikel 87 i forordningen. I det omfang at niveauet for sikkerhedskravene vedr. CPR-numre ikke er klart specificeret juridisk medfører dette en risiko for misforståelser. Det ville derfor være hensigtsmæssigt, hvis CPR-nummerets status angives i loven, således at kravene til niveauet for beskyttelse ikke kan give anledning til tvivl.

Bestemmelsen vurderes derudover ikke at stille Moderniseringsstyrelsen anderledes end i dag.

B. Indsigtsret i forbindelse med statistiske undersøgelser, jf. § 22
I udkastet til den nye databeskyttelseslov, står der i § 22, stk. 5 under kapitlet om begrænsning af den registreredes rettigheder (vedrørende indsigt), at: ”*Databeskyttelsesforordningens artikel 15, stk. 1, finder ikke anvendelse, hvis oplysningerne udelukkende behandles i videnskabeligt øjemed, eller hvis oplysningerne kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker*”.

Ovenstående udnytter ikke fuldt ud mulighederne i forordningen for at begrænse registreredes indsigtsret. Den danske bestemmelse undtager kun registreredes rettigheder efter en enkelt af de mulige bestemmelser, ligesom bestemmelsens anvendelsesområde (*"videnskabeligt øjemed"*), synes mere begrænset en forordningen giver mulighed for ("*videnskabelige eller historiske forskningsformål eller til statistiske formål*", jf. artikel 89). Denne danske begrænsning kan have negative konsekvenser for Moderniseringsstyrelsen - og vores samarbejdspartneres - muligheder for statistisk at understøtte arbejdsmarkeds- og overenskomstområdet. Dansk Arbejdsgiverforening har fx skrevet til MODST, at de er bekymret over formuleringen i § 22, stk. 5.

Justitsministeriet bør på den baggrund overveje at udvide anvendelsesområdet for § 22, stk. 5. Det afgørende for MODST er i den forbindelse, at "*videnskabelige eller historiske forskningsformål eller til statistiske formål*" kommer til at fremgå af den nævnte undtagelsesbestemmelse på en måde, således at det statistiske arbejde i forbindelse med overenskomstforhandlinger m.m. undtages.

C. Præcisering af regel om høring af Datatilsynet ved udarbejdelse af generelle retsforskrifter, jf. § 28

Det fremgår af udkastet til databeskyttelseslovens § 28, at der skal foretages høring af Datatilsynet ved udarbejdelse af bl.a. cirkulærer, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger.

Bestemmelsens ordlyd er overvejende identisk med den gældende persondatalovs § 57. Af betænkning nr. 1345/1997 om persondataloven, s. 369, fremgår om bestemmelsen i den gældende persondatalov: *"myndighedens dispositioner af privatretlig karakter, f.eks. indgåelse af kontrakter eller indgåelse af kollektive aftaler på det arbejdsretlige område, må antages at falde uden for [§ 57]"*.

Moderniseringsstyrelsen finder på den baggrund, at det vil være hensigtsmæssigt, at der i bemærkningerne til den foreslåede § 28 anføres følgende: *"Dispositioner af privatretlig karakter, f.eks. indgåelse af kontrakter eller indgåelse af kollektive aftaler på det arbejdsretlige område, er ikke omfattet af § 28*." Dermed vil der i det nye lovgrundlag forsat ikke være tvivl om, at der ikke skal ske høring hos Datatilsynet i forbindelse med udbud og indgåelse af kollektive aftaler.

Patientdataforeningen, 20. august 2017.

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

Patientdataforeningen tillader sig hermed at indsende høringssvar uden at være på den offentlige høringsliste. Det gør vi grundet den omfattende betydning lovforslaget, hvis det vedtages, vil få for den danske befolkning og retten til beskyttelse af helt private og intime persondata.

Databeskyttelsesloven kan ses som en dansk fortolkning af EU Persondataforordningen, og er beregnet til at eksistere parallelt med Forordningen. Patientdataforening finder suppleringsloven alt for vidtgående og, trods den fine titel, stort set i direkte modstrid med det oprindelige formål med Persondataforordningen. Men kan sat på spidsen sige, at danskerne med Databeskyttelsesloven vil blive noget nær retsløse på persondataområdet

Baggrund og perspektiv
Danmarks tilgang til tvungen dataregistrering og deling af følsomme persondata uden samtykke er forældet og udemokratisk, og lande som Estland giver nu Danmark baghjul (1). Danmark har i snart mange år, i et utvivlsomt velment forsøg på at gøre Danmark attraktiv for medicinalvirksomheder og førende indenfor registerforskning, i høj grad tilsidesat borgernes ret til privatlivsbeskyttelse, i sådan en grad at man tilsyneladende ikke har bemærket, at der i stigende grad internationalt er fokus på nye og tidssvarende løsninger i forbindelse med digitalisering af persondata.

Lande som Estland har til gengæld længe været i front med implementering af nye borgernære løsninger for datadeling, omend esterne med deres *block-chain* løsning ikke er helt i mål med *privacy-by-design* (2). I forhold til infrastruktur og demografi ligner Estland og Danmark hinanden. Men i Danmark er vi netop nu ved at vedtage en Databeskyttelseslov, der gør at vi lynhurtigt vil sakke bagud. Vi har altså med stor sandsynlighed tabt det digitale kapløb, inden det rigtigt kom i gang.

I stedet burde vi være visionære og udnytte særlige danske styrker. I Danmark har vi 50 års erfaring med offentlig dataindsamling, en befolkning som har stor tillid til dataindsamling og endnu ikke har udviklet den helt store aversion mod "big-brother", et moderne digitaliseret sundhedsvæsen og en stærk medicinalindustri. Danmark har derfor alle muligheder for lynsnart, at lægge sig forrest når det gælder brug af følsomme persondata og sundhedsdata især. Men det kræver at vi forlader et forældet princip om registreringstvang.

Lægeforeningen har modigt tiltrådt Taipei deklarationen (3) om moderne håndtering af sundhedsdata og biomateriale. Det er i deklarationen et hovedprincip, at patienternes værdighed, autonomi og privatliv bedst beskyttes ved at inddrage patienterne i beslutning om brug af deres sundhedsdata. Taipei-deklarationen åbner i modsætning til den danske suppleringslov ikke op for, at myndighederne kan udhule og ophæve de grundlæggende patientrettigheder om inddragelse og selvbestemmelse. Det er Patientdataforeningens store bekymring at Folketinget med suppleringsloven er ved at skrive Danmark ud af en international forskningstradition.

Danske forskere vil fremover risikere ikke at kunne dokumentere, at de overholder Taipei Deklarationens grundlæggede rettigheder, hvorfor dansk forskning i andre lande vil blive betragtes som uetisk og fremover ikke vil kunne publiceres internationalt. Der er allerede i dag i international sammenhæng samtykkebaserede

forskningsdatabaser med mere end 5 millioner registrerede, som udsætter de danske registre for betydelig etisk konkurrence.

Overordnede kommentarer til den foreslåede suppleringslov

1. **Kompliceret og uanvendelig**
   Lovforslag er meget langt og kompliceret og breder sig over 324 sider. Det er et indlysende problem, fordi mange helt almindelige borgere skal kunne forholde sig til loven. Ved at inddrage 324 sider får man i den danske suppleringslov plads til at udnytte hele Forordningens elasticitet udelukkende med det formål at udvande privatlivsbeskyttelsen.

2. **Manglende samtykke og beskyttelse af privatliv**
   Forordningen tillader ikke behandling af følsomme personoplysninger, med mindre der foreligger et samtykke, eller data er omfattet af nogle konkrete undtagelser. Det fremgår af Forordningens artikel 9. Det er samtidig klart, at forordningen ikke kun tillader, men også tilskynder til, at man i national lovgivning indbygger retsgarantier, der beskytter den enkelte borger. Samtykke giver en langt stærkere borgerbeskyttelse end de andre undtagelser.

   Hver gang man lader et område for persondatabehandling regulere af andre undtagelser end samtykke, så bevæger man sig væk fra borgernes ret til selvbestemmelse og beskyttelse af privatlivet. I Danmark har vi over 100 sundhedsregistre, som tilsammen duplikerer indholdet af borgernes patientjournal. Der er for langt størstedelen af registrene tvang når det gælder indberetning, idet hverken fagpersoner eller patienter kan modsætte sig indberetning.

   Når data først ligger i et register kan data i personhenførbar form deles videre. Man kunne med Databeskyttelsesloven have valgt at regulere datatrafikken med samtykke. I stedet har man valgt at regulere vha. en konkret undtagelse. Derved ophører retten til privatliv og selvbestemmelse. I demokratiske lande vi normalt sammenligner os med findes registreringstvang ikke. Her tillader man samtykke inden brug af behandlingsdata til sekundære formål så som forskning.

   Med den nye EU Persondataforordning og den danske Databeskyttelseslov havde der været en oplagt mulighed for at sikre danske borgere den demokratiske ret til selvbestemmelse, men igen vælger vi i Danmark forældet og paternalistisk registreringstvang. De øvrige EU-lande vil næppe kunne spejle sig i den danske suppleringslov, som understreger den danske enegang, når det gælder manglende demokratisk selvbestemmelse over persondata. Det grundlæggende spørgsmål er derfor, hvorfor skal danske borgere stilles dårligere end borgere i andre demokratiske lande?

3. **Principper for dataminimering, privacy-by-design og privacy-by-default er elastik i metermål**
   Principperne, der sikrer *dataminimering*, *privacy-by-default* og *privacy-by-design*, bør defineres og stadfæstes detaljeret og tydeligt i Databeskyttelsesloven, ellers bliver de, især i forhold til dataansvarliges egen risikovurdering, alt for elastiske og giver ingen reel beskyttelse for borgerne. På disse områder fremstår suppleringsloven ufærdig.

   Der har i dansk lovgivningen været en årelang og beklagelig tradition for at udelade tekniske krav til at behandle personoplysninger, der bedst sikre privatlivsbeskyttelse. Det har været en sovepude

for myndighederne, som i deres systemudvikling har undladt at tænke i beskyttelse af borgernes integritet. Konsekvenserne har været at telefonmedarbejdere i sygehusets reception, ansatte lærere og socialrådgivere har haft adgang til patientjournalerne på lige fod med det sundhedsfaglige personale, og at adgang til logning i de fleste sammenhænge ikke har været mulig.

4. **Offentlige myndigheder sættes over loven**
   Det fremgår af lovforslagets § 41, stk. 5, at afklaring i forhold til sanktioner for offentlige myndigheder udestår. Er der ikke risiko for sanktion for offentlige myndigheder forstærkes problemerne i forhold til den i forvejen ret ekstreme danske fortolkning af Forordningen, og det offentligt kan i realiteten lade persondata sejle.

Konkrete bemærkninger i relation til paragraffer

5. **Formålsskred**
   Der er som nyt i §5 i forslag til suppleringslov åbnet op for, at myndighederne, i administrativt fastsatte regler, selv kan sætte rammerne for hvornår oplysninger indsamlet til behandling kan viderebehandles til andre formål.

   Det gør at problemerne om at overholde det såkaldte *finalité*-princip – princippet om formålsbestemthed – i dansk retspraksis forværres. Det har gennem en årrække været en uskik i Danmark først at indsamle data med et formål for siden at udvide formålet til noget helt andet. Det så man blandt andet i forbindelse med den ulovlige DAMD database, hvor et af problemerne var et formålsskred. I en rapport fra SSI dokumenteredes det, at alle centrale aktører og myndigheder var bekendt med, at oplysninger ulovligt blev behandlet til andre formål end de oprindelige og fortsatte uagtet det massive misbrug af danskernes helbredsoplysninger. En sådan praksis kan nu lovliggøres med en administrativ bekendtgørelse. Patientdataforeningen skal minde om, at mere end 30.000 danskere aktivt bad om at blive slettet fra databasen.

   Formålsfordrejning umuliggør gennemsigtighed, for hvordan skal borgerne kunne informeres om formålet med indsamling af data hvis formålet siden ændres? Muligheden for formålsskred formaliseres nu og endda så det kan reguleres rent administrativt. Det åbner for uhørte frihedsgrader for at samkøre data, hvor der tidligere var helt vandtætte skotter. I realiteten er Danmark, når det gælder persondata, reduceret til et teknokrati.

6. **Kontrolformål**
   Der er som nyt i §6 og §9 i forslag til suppleringslov åbnet op for, at myndighederne kan samkøre og sidestille oplysninger om borgernes private, økonomiske, sociale og helbredsmæssige forhold til brug for kontrolformål. Det kan i modsætning til hvad, der gælder i dag ske uden udtrykkelig hjemmel i lov, uden patienten informeres og uden Datatilsynets godkendelse. Suppleringsloven åbner derved op for vidtgående samkøring af oplysninger, samtidig med at det er op til myndighederne selv at afgøre, hvad der skal kontrolleres og hvordan.

7. **Samfundsmæssig interesse**
   Der er som noget nyt i suppleringslovens §9 foreslået, at myndighederne kan behandle og dele oplysninger af hensyn til væsentlige samfundsmæssige interesser. Det er som noget nyt

myndigheden selv, der afgør, om deres eget formål har en væsentlige samfundsmæssig interesse, og der er heller ikke her krav om udtrykkelig hjemmel i lov, oplysningspligt eller forudgående godkendelse fra Datatilsynet. De særlige indtagelser gælder kun for offentlige myndigheder. Det er patientdataforeningens opfattelse, at suppleringsloven gør urimelig forskel på private virksomheder og offentlige myndigheder, og der er endelig patientdataforeningens opfattelse, at kravene om noget bør være skærpet for offentlige myndigheder, der er de suverænt største data-behandlere og de databehandlere med flest sager om misbrug af oplysninger.

MVH

Formand for Patientdataforeningen, Thomas Birk Kristiansen (Repræsenterer ca. 100 læger og 1000 patienter)

Referencer

1) http://pwc.blogs.com/health_matters/2017/03/estonia-prescribes-blockchain-for-healthcare-data-security.html
2) https://www.corda.net/2017/02/corda-way-thinking/
3) https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/

Fra: Jan Hempel [Jan.Hempel@politiforbundet.dk]
Sendt: 10. juli 2017 08:09
Til: Justitsministeriet
Emne: VS: Høring over udkast til forslag til databeskyttelsesloven - (2016-7910-0021)
Vedhæftede filer: Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelseslo [DOK2365818].pdf; Høringsliste [DOK2294269].pdf; Høringsbrev DOK2346800.pdf; fesdPacket.xml

Til Justitsministeriet.

Politiforbundet har ingen bemærkninger til lovforslaget.

Politiforbundets jr.nr. 2017-00538.

På forbundets vegne - og med venlig hilsen

Jan Hempel
Forbundssekretær

H.C. Andersens Boulevard 38
DK-1553 København V

Tlf. +45 3345 5900
E-mail mail@politiforbundet.dk

Fra: Justitsministeriet [mailto:jm@jm.dk]
Sendt: 7. juli 2017 14:09
Til: pibr@domstol.dk; hoeringer@dommerfm.dk; $Direktoratet for Kriminalforsorgen <dfk@kriminalforsorgen.dk>; dkr@dkr.dk; office@voldgiftsinstituttet.dk; dch@dch.dk; dommerforeningen@gmail.com; dt@datatilsynet.dk; kontakt@danskeudlejere.dk; info@danske-seniorer.dk; regioner@regioner.dk; mail@danskemedier.dk; forening@danskeadvokater.dk; dh@handicap.dk; cbh@danskeforlag.dk; mail@danskeadvokater.dk; info@danske-aeldreraad.dk; dj@journalistforbundet.dk; dit@dit.dk; adm@nodeco.dk; di@di.dk; dfs@dfs.dk; hoeringssager@danskerhverv.dk; de@de.dk; info@danskbyggeri.dk; da@da.dk; dtu@dtu.dk; journalen@dr.dk; dl@dklf.dk; djoef@djoef.dk; dif@dif.dk; bl@bl.dk; cbs@cbs.dk; Socialmin. <sm@sm.dk>; raadhus@99454545.dk; brondby@brondby.dk; post@brk.dk; bl@bl.dk; kommunen@billund.dk; Beskæftigelsesmin. <bm@bm.dk>; balkom@balk.dk; pote@atp.dk; assens@assens.dk; mail@arkitektforeningen.dk; ae@ae.dk; abf@abf-rep.dk; amnesty@amnesty.dk; Allerød Kommune <kommunen@alleroed.dk>; albertslund@albertslund.dk; ac@ac.dk; samfund@advokatsamfundet.dk; ekspedition.law@au.dk; post@aarhusretshjaelp.dk; post@aarhus.dk; law@law.aau.dk; Aalborg Kommune – Folkeregisteret <aalborg@aalborg.dk>; post@aabenraa.dk; 3f@3f.dk; post@oestrelandsret.dk; oim@oim.dk; post@aeroekommune.dk; aef@aeldreforum.dk; aeldresagen@aeldresagen.dk; post@vordingborg.dk; viborg@viborg.dk; post@vestrelandsret.dk; post@vesthimmerland.dk; Vejle Kommune <post@vejle.dk>; post@vejenkom.dk; vardekommune@varde.dk; raadhus@vallensbaek.dk; uvm@uvm.dk; uim@uim.dk; um@um.dk; ufm@ufm.dk; hfa@ac.dk; Tårnby

Kommune <kommunen@taarnby.dk>; toender@toender.dk; jura@tv2.dk; trm@trm.dk; ssha@domstol.dk; thistedkommune@thisted.dk; post@sonderborg.dk; post@shret.dk; Syddjurs Kommune <syddjurs@syddjurs.dk>; sdu@sdu.dk; svendborg@svendborg.dk; sum@sum.dk; struer@struer.dk; stevns@stevns.dk; stm@stm.dk; Sorø Kommune <soroekom@soroe.dk>; kommune@solrod.dk; slagelse@slagelse.dk; Skive Kommune <sk@skivekommune.dk>; skm@skm.dk; Skanderborg Kommune <skanderborg.kommune@skanderborg.dk>; kommunen@silkeborg.dk; ksm@sikkerhedsbranchen.dk; Samsø Kommune <kommune@samsoe.dk>; slrtv@slrtv.dk; rem@siri.dk; info@digitalsikkerhed.dk; Rødovre Kommune <rk@rk.dk>; rudersdal@rudersdal.dk; kommunen@roskilde.dk; ringsted@ringsted.dk; post@rksk.dk; politi@politi.dk; ro@fo.stm.dk; riomgr@gl.stm.dk; rigsadvokaten@ankl.dk; frederiksberg@domstol.dk; bornholm@domstol.dk; viborg@domstol.dk; sonderborg@domstol.dk; svendborg@domstol.dk; roskilde@domstol.dk; randers@domstol.dk; odense@domstol.dk; naestved@domstol.dk; nykobing@domstol.dk; lyngby@domstol.dk; kolding@domstol.dk; horsens@domstol.dk; holstebro@domstol.dk; holbaek@domstol.dk; hjorring@domstol.dk; hillerod@domstol.dk; herning@domstol.dk; helsingor@domstol.dk; glostrup@domstol.dk; esbjerg@domstol.dk; aarhus@domstol.dk; aalborg@domstol.dk; formand@retspolitik.dk; info@shipowners.dk; raadhus@rebild.dk; rkr@rkr.dk; mail@realkreditforeningen.dk; randerskommune@randers.dk; prosa@prosa.dk; post@procesbevillingsnaevnet.dk; skrivpost@postnord.com; Politiforbundet <mail@politiforbundet.dk>; lfr001@politi.dk; sekretariat@parcelhus.dk; Odsherred Kommune <kommune@odsherred.dk>; Odense Kommune <odense@odense.dk>; odder.kommune@odder.dk; borger@naestved.dk; kommune@nyborg.dk; Nordfyns Kommune <post@nordfynskommune.dk>; norddjurs@norddjurs.dk; nmkn@nmkn.dk; kommunen@morsoe.dk; fmn@fmn.dk; pibr@domstol.dk; hoeringer@dommerfm.dk; $Direktoratet for Kriminalforsorgen <dfk@kriminalforsorgen.dk>; dkr@dkr.dk; office@voldgiftsinstituttet.dk; dch@dch.dk; dommerforeningen@gmail.com; dt@datatilsynet.dk; kontakt@danskeudlejere.dk; info@danske-seniorer.dk; regioner@regioner.dk; mail@danskemedier.dk; forening@danskeadvokater.dk; dh@handicap.dk; cbh@danskeforlag.dk; mail@danskeadvokater.dk; info@danske-aeldreraad.dk; dj@journalistforbundet.dk; dit@dit.dk; adm@nodeco.dk; di@di.dk; dfs@dfs.dk; hoeringssager@danskerhverv.dk; de@de.dk; info@danskbyggeri.dk; da@da.dk; dtu@dtu.dk; journalen@dr.dk; dl@dklf.dk; djoef@djoef.dk; dif@dif.dk; bl@bl.dk; cbs@cbs.dk; Socialmin. <sm@sm.dk>; raadhus@99454545.dk; brondby@brondby.dk; post@brk.dk; bl@bl.dk; kommunen@billund.dk; Beskæftigelsesmin. <bm@bm.dk>; balkom@balk.dk; pote@atp.dk; assens@assens.dk; mail@arkitektforeningen.dk; ae@ae.dk; abf@abf-rep.dk; amnesty@amnesty.dk; Allerød Kommune <kommunen@alleroed.dk>; albertslund@albertslund.dk; ac@ac.dk; samfund@advokatsamfundet.dk; ekspedition.law@au.dk; post@aarhusretshjaelp.dk; post@aarhus.dk; law@law.aau.dk; Aalborg Kommune – Folkeregisteret <aalborg@aalborg.dk>; post@aabenraa.dk
Emne: Høring over udkast til forslag til databeskyttelsesloven - (2016-7910-0021)

Se vedhæftede bilag.

Med venlig hilsen

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

Fra: Sten Schaumburg-Müller [stsm@sam.sdu.dk]

Sendt: 22. august 2017 10:16

Til: £Databeskyttelseskontoret (951s26)

Emne: Databeskyttelseslov - Høringssvar

Vedhæftede filer: jur_2017_2_03.pdf

Til databeskyttelseskontoret

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

Som juridisk forsker vil jeg gerne påpege nogle problemer ved det fremsendte forslag:

- De foreslåede regler giver ligesom de aktuelle regler i persondataloven en bloc-undtagelse til al journalistik i stedet for den foreskrevne gennemtænkte afbalancering.

- De foreslåede regler giver ligesom den aktuelt gældende persondatalov forrang for ytrings- og informationsfriheden i stedet for den krævede »forening« af de til tider modsatrettede hensyn.

- De foreslåede regler er ligesom de aktuelt gældende regler i persondataloven og mediedatabaseloven til tider diskriminerende over for ikke-danske aktører og dermed i strid med EU-retten.

- Det gældende krav i mediedatabaseloven om sletning af 3 år gamle oplysninger er ikke i god overensstemmelse med forordningens art. 85.

- Hertil kommer, at det bør overvejes, om undtagelserne fra persondataforordningens regler ved journalistisk virksomhed bør gælde i samme omfang for professionelle medier, der er underlagt vejledende regler om god presseskik og Pressenævnets kompetence, som for ikke-professionelle medier, der så hverken skal følge professionelle standarder eller persondataretlige regler. Virkningen synes at være en styrkelse a potentielle fake news-medier vis-a-vis professionelle medier.

Jeg vedlægger »Persondatabehandling i journalistisk øjemed«, trykt i Juristen, 2017, nr. 2, s. 53-62, for en nærmere analyse og argumentation. Artiklen er skrevet af professor Søren Sandfeld Jakobsen og undertegnede.

Venlig hilsen

Sten Schaumburg-Müller
Professor, dr.jur.
Juridisk Institut

T 65 50 82 41
M 31 72 43 32
stsm@sam.sdu.dk
www.sdu.dk/ansat/stsm

Syddansk Universitet
Campusvej 55
5230 Odense M
www.sdu.dk

alt="http://cdn.sdu.dk/img/sdulogos/SDU_BLACK_signatur.png" border=0>

Til: databeskyttelseskontoret@jm.dk

København d. 2017-08-22

Høring over udkast til forslag til databeskyttelsesloven

PROSA finder mange gode tiltag i EU's Persondataforordning.

Et af problemerne ved persondata er administrationen af informeret samtykke. Her vil PROSA gerne slå til lyd for, at Danmark for udarbejdet en digital service, hvor borgerne kan give og tilbagekalde samtykke. Dette må gerne foregå som meta-samtykker, hvor man giver samtykke til en hel gruppe af data og formål.

Servicen bør også kunne give borgerne en oversigt over, hvor de er registrerede.

Vi kan derudover bakke op om høringssvarene fra IDA, Forbrugerrådet Tænk, Patientdataforeningen, Institut for Menneskerettigheder og Rådet for Digital Sikkerhed.

Venlig hilsen

Niels Bertelsen
Formand for PROSA

Justitsministeriet
Lovafdelingen
Databeskyttelseskontoret

Mail: databeskyttelseskontoret@jm.dk

23. august 2017

Vedr. Sagsnr. 2016-7910-0008

HØRINGSSVAR OM UDKAST TIL FORSLAG TIL DATABESKYTTELSESLOVEN

Red Barnet takker for muligheden for at udtale sig om Databeskyttelseskontorets udkast til Databeskyttelsesloven. Red Barnet vil i sine kommentarer kun fokusere på den artikel, som har særlig relevans for børn og unge.

Red Barnet kan tilslutte sig Justitsministeriets forslag om, at der i artikel 8 fastsættes en aldersgrænse på 13 år for børns samtykke til anvendelse af informationssamfundstjenester.

For børn og unge i Danmark har adgangen til informationer via hjemmesider, søgemaskiner og gennem deltagelse i online aktiviteter stor samfundsmæssig og social betydning. Aktiviteter i denne sammenhæng er med til at skabe og fastholde kontakt med kammerater, deltage i forskellige diskussionsfora, søge information til skolearbejde, spille spil, se film og lytte til musik.

Gennem flere år har vi i Red Barnet kunnet konstatere, at også børn yngre end 13 år opretter egne profiler på sociale medier, selvom dette er i konflikt med udbydernes regler. Udfordringen med denne gruppe af børn er, at de hemmeligholder deres aktiviteter i forhold til forældre og fagpersoner, fordi de er klar over, at de bryder nogle regler. En højere aldersgrænse for, hvornår et barn gyldigt kan give samtykke til behandling af personoplysninger vil blot føre til, at endnu flere børn og unge vil være til stede i onlinemiljøer i hemmelighed. Dermed mindskes mulighederne og sandsynlighederne for, at disse børn og unge vil søge hjælp og støtte, når de oplever mobning, chikane, trusler og overgreb.

Det er Red Barnets erfaring, at det ikke er muligt i tilstrækkelig grad at regulere og kontrollere børnenes online adfærd, hverken gennem tekniske foranstaltninger (filtre og overvågningsprogrammer) eller gennem strammere bestemmelser. Den bedste beskyttelse af børnene opnås gennem åben dialog med dem om udfordringer og risici. At fastholde en aldersgrænse på 13 år er vigtig, idet den signalerer, at brugen af online profiler og tjenester kræver en vis alder og modenhed. Samtidig er der stor forskel på børns modenhed og

Red Barnet
Rosenørns Allé 12
1634 København V
Danmark

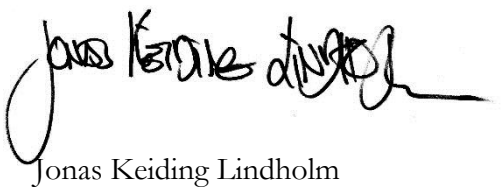
Telefon 35 36 55 55
Fax 35 39 11 19
redbarnet@redbarnet.dk
www.redbarnet.dk

ansvarsfølelse, men generelt vil 13 års alderen være det tidspunkt i barnets udvikling, hvor man hos de fleste børn kan forvente en selvstændig og reflekteret brug af online profiler og tjenester.

Det forudsætter dog stadig, at der sker en høj prioritering af undervisning til fagfolk, børnene selv og deres forældre om, hvordan børn bedst støttes i at udvikle en god net-etik kombineret med viden om digitale rettigheder, databeskyttelse og risici for digitale krænkelser i form af mobning, chikane, trusler og overgreb.

Red Barnet stiller sig gerne til rådighed i forhold til at uddybe kommentarerne til høringen. Faglig kontaktperson: Psykolog Kuno Sørensen, ks@redbarnet.dk, tlf. 25140069.

Med venlig hilsen



Jonas Keiding Lindholm
Generalsekretær

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 22. august 2017

JOURNAL NR.
RA-2017-3200604-30

SAGSBEHANDLER: JSB/

Høring over udkast til databeskyttelseslov

Ved e-mail af 7. juli 2017 (sagsnr. 2016-7910-0021) har Justitsministeriet anmodet om Rigsadvokatens eventuelle bemærkninger til udkast til forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

I den anledning skal jeg bemærke følgende:

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

Databeskyttelsesforordningens artikel 6, litra e, fastslår, at en behandling bl.a. er lovlig, hvis den er nødvendig af hensyn til udførelse af en opgave, som henhører under offentlig myndighedsudøvelse. Det følger videre af forordningens artikel 6, litra f, at en behandling som udgangspunkt er lovlig, hvis den er nødvendig for, at den dataansvarlige eller tredjemand kan forfølge en berettiget interesse. Efter andet led i litra f finder første led af bestemmelsen imidlertid ikke anvendelse i relation til behandling i forbindelse med myndighedsudøvelse.

Det kan efter min opfattelse med fordel nærmere beskrives i lovudkastets bemærkninger, om konsekvensen heraf er, at "berettiget interesse"-hjemlen (smh. § 6, stk. 1, nr. 7, i den nugældende persondatalov), herefter ikke længere kan anvendes til behandling af oplysninger, der sker i forbindelse med udførelsen af myndighedens opgaver, og om

myndighedens behandling derfor i stedet vil skulle ske på baggrund af øvrige hjemler, herunder "offentlig myndighedsudøvelse/en opgave i samfundets interesse"-hjemlen (smh. § 6, stk. 1, nr. 5 og 6 i den nugældende persondatalov) - også i forbindelse med behandling af personoplysninger hos myndigheder, der er kompetente myndigheder efter lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger, men på områder der i øvrigt falder uden for retshåndhævelseslovens anvendelsesområde. Spørgsmålet om rette hjemmel kan eksempelvis opstå i relation til personaleadministration, særligt i forhold til tilfælde hvor forordningens artikel 6, stk. 1, litra b, ikke er anvendelig, eller i forbindelse med registrering af pressehenvendelser, vidensdeling mv.

2. Det følger af lovudkastets § 41, at overtrædelse af forordningen, databeskyttelsesloven eller regler udstedt i medfør heraf straffes med bøde eller fængsel indtil 6 måneder. Jeg skal i den forbindelse bemærke, at den angivne strafferamme indebærer, at sådanne overtrædelser forældes efter 2 år, jf. straffelovens § 93, og at strafferammen vil betyde visse begrænsninger i, hvilke efterforskningsmidler og straffeprocessuelle tvangsindgreb der kan bringes i anvendelse ved behandlingen af sådanne sager.

3. Det skal bemærkes, at Rigsadvokaten ikke har vurderet de økonomiske konsekvenser af lovudkastet, men forventer at blive inddraget i disse spørgsmål senere i forløbet.

Med venlig hilsen

Jeanie Sølager Bigler
Vicestatsadvokat

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendt pr. e-mail til:
databeskyttelse@jm.dk

J.nr.: 2017-000-41
Sagsbehandler: Christian Tolstrup Lund

RIGSPOLITIET
FORVALTNINGSRETS-
CENTRET
POLITITORVET 14
1780 KØBENHAVN V

Telefon: 3314 8888

Web: www.politi.dk

Justitsministeriets høring over udkast til forslag til databeskyttelseslov – Ministeriets sags.nr. 2016-7910-0021

Justitsministeriet har den 7. juli 2017 anmodet om bemærkninger til forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

1. Lovens materielle anvendelsesområde

Det fremgår af lovforslagets § 1, stk. 2, 2. pkt., at lovforslaget og databeskyttelsesforordningen ikke gælder i det omfang, der er nævnt i databeskyttelsesforordningens[1] artikel 2, stk. 2, litra b-d.

I de specielle bemærkninger til lovforslagets § 1, stk. 2, fremgår det, at Justitsministeriet finder, at det med fremgangsmåden slås fast, at forordningen vil gælde på alle livsområder med undtagelse af bl.a. de områder, der er nævnt i forordningens artikel 3, stk. 2, litra d. Rigspolitiet går ud fra, at der rettelig skal henvises til forordningens artikel 2, stk. 2, litra d.

Justitsministeriet henviser desuden nærmere til lovforslagets almindelige bemærkninger afsnit 2.1 og til betænkning nr. 1564 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning.

Følgende fremgår bl.a. af de almindelige bemærkninger pkt. 2.1.2:

[1] Europa-parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

"Og endelig gælder forordningen efter artikel 2, stk. 2, litra d, ikke for behandling af personoplysninger, som foretages for kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

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

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

Det er Rigspolitiets opfattelse, at det bør fremgå udtrykkeligt af databeskyttelsesloven, at loven ikke finder anvendelse på behandling af personoplysninger, der er omfattet af retshåndhævelsesloven[2]. Rigspolitiet tillægger det i den forbindelse navnlig betydning, at afgrænsningen af hvad der i dansk ret udgør en kompetent myndighed følger af retshåndhævelsesloven, og ikke i sig selv kan udledes af databeskyttelsesforordningens artikel 2, stk. 2, litra d.

2.1. Generelle forhold knyttet til videregivelse af personoplysninger til politiet

Generelt i forhold til spørgsmålet om videregivelse af personoplysninger skal Rigspolitiet bemærke, at indsamling af oplysninger – herunder personoplysninger – er et essentielt redskab i forbindelse med løsning af politiets kerneopgaver. Kvaliteten af politiets arbejde og sagsbehandlingstiden afhænger således i høj grad af mængden og karakteren af de oplysninger, som politiet behandler.

Politiet oplever imidlertid i stigende omfang, at private og offentlige dataansvarlige – ofte under påberåbelse af databeskyttelsesretten – er tilbageholdende med at videregive personoplysninger til politiet bl.a. som led i en anmeldelse af strafbare forhold.

Det er Rigspolitiets opfattelse, at personoplysninger kan videregives til politiet som led i anmeldelser af strafbare forhold inden for den nugældende databeskyttelsesretlige regulering, når blot der er en helt umiddelbar indikation af, at videregivelsen vil kunne have relevans for politiets efterforskning af et strafbart forhold,

[2] Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandlings af personoplysninger

jf. nærmere herom nedenfor. Efter dansk ret må den retlige ramme for, hvornår en anmeldelse af et strafbart forhold må anses for uberettiget således antages at være fastsat ved straffelovens § 165 om falsk anmeldelse mv.

Ved anmeldelser af strafbare forhold efter gældende ret videregives der således eksempelvis ganske betydelige mængder – bl.a. følsomme – personoplysninger til politiet. Dette sker bl.a. til brug for sager af lav strafværdighed og sager, hvor der alene er tale om en mistanke, der kun er underbygget i begrænset omfang med henblik på, at politiet træffer beslutning om at indlede videre efterforskning mv., jf. retsplejelovens § 742.

Det kan efter Rigspolitiets opfattelse ikke antages, at hverken persondataloven eller databeskyttelsesforordningen har til formål at begrænse adgangen til at indføre eller opretholde en ordning af strafferetsplejen svarende til den ovenfor beskrevne.

Det er herefter Rigspolitiet opfattelse, at det udtrykkeligt bør fremgå af lovforslaget, at en videregivelse af enhver personoplysning til politiet kan finde sted inden for rammerne af databeskyttelsesforordningen og lovforslaget, når dette sker som led i en anmeldelse af et strafbart forhold. Det bør i den forbindelse ligeledes fremgå, at der uden for de tilfælde, hvor oplysninger videregives til politiet som led i en anmeldelse af strafbare forhold, vil kunne videregives personoplysninger – f.eks. som led i et løbende kriminalpræventivt samarbejde – i overensstemmelse med gældende ret, herunder databeskyttelsesforordningen og databeskyttelseslovens bestemmelser. De nærmere overvejelser om disse spørgsmål fremgår i det følgende.

2.1.1. Lovforslagets regulering af videregivelse af personoplysninger til politiet

Lovforslaget sondrer mellem behandling af *almindelige personoplysninger* (lovforslagets § 6), behandling af *følsomme personoplysninger* (lovforslagets § 7) og behandling af oplysninger om strafbare forhold (lovforslagets § 8).

2.1.2. Almindelige personoplysninger

For så vidt angår almindelige personoplysninger er det Rigspolitiets opfattelse, at *offentlige myndigheder* efter omstændighederne kan videregive sådanne oplysninger til politiet efter databeskyttelsesforordningens artikel 6, stk. 1, litra c (nødvendig behandling med henvisning til en retlig forpligtelse) eller e (hensynet til udfø-

relse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse).

For så vidt angår *privates* videregivelse af personoplysninger til politiet vil dette efter Rigspolitiets opfattelse kunne ske efter artikel 6, stk., litra c, (når der foreligger en indberetningspligt, en retskendelse mv.) eller værdispringsreglen i forordningens artikel 6, stk. 1, litra f.

Rigspolitiet finder herefter, at spørgsmålet om adgangen til at videregive almindelige *ikke-følsomme* personoplysninger til politiet som led i anmeldelse af strafbare forhold, ikke bør give anledning til tvivl. Med henblik på at undgå enhver tvivl herom, skal det dog anbefales, at adgangen til at videregive disse oplysninger beskrives generelt i lovforslaget, og at der i relevant omfang redegøres for overvejelser svarende til det under punkt 2.1. anførte.

2.1.3. Følsomme personoplysninger

Videregivelse af følsomme personoplysninger fra *offentlige myndigheder* kan efter Rigspolitiets opfattelse ske til politiet efter lovforslagets § 7, stk. 4, hvorefter behandling af følsomme personoplysninger kan ske, hvis behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser. Dette bør efter Rigspolitiets opfattelse fremgå af bemærkningerne til bestemmelsen. For så vidt angår *privates* videregivelse af følsomme personoplysninger til politiet henvises der til punkt 2.2. nedenfor.

2.1.4. Oplysninger om strafbare forhold

Efter lovforslagets § 8, stk. 1, må der for den *offentlige forvaltning* ikke behandles oplysninger om strafbare forhold, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver.

Videre følger det af lovforslagets § 8, stk. 2, at de oplysninger, der er nævnt i stk. 1, i udgangspunktet ikke må videregives. Videregivelse kan dog ske under visse betingelser, bl.a. hvis videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår, eller hvis videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe.

For så vidt angår *private* fremgår det af lovforslagets § 8, stk. 3, at private må behandle oplysninger om strafbare forhold, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Desuden må private behandle sådanne oplysninger, hvis det er nødvendigt til varetagelsen af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede.

2.2. Sammenfatning og anbefaling

I forhold til *privates* videregivelse af *følsomme personoplysninger* omfattet af databeskyttelsesforordningens artikel 9, stk. 1, bemærkes det, at denne ikke ses at kunne finde sted i medfør af lovforslagets § 7, stk. 4, idet dette forudsætter tilladelse fra Datatilsynet. På denne baggrund skal det anbefales, at der i overensstemmelse med forordningens artikel 9, stk. 2, litra g, udtrykkeligt fastsættes bestemmelse om, at sådanne oplysninger kan videregives til politiet som led i indgivelsen af en anmeldelse af strafbart forhold. Det bemærkes i den forbindelse, at det fremgår af lovforslagets bemærkninger, at bl.a. databeskyttelsesforordningens artikel 9, stk. litra g, forudsætter, at behandlingen er forankret f.eks. i national ret.

Alternativt – eller som supplement – kan det overvejes, om det i bemærkningerne til lovforslagets § 7, stk. 1, kan anføres, at bestemmelsen i databeskyttelsesforordningens artikel 9, stk. 2, litra f, vil kunne danne grundlag for videregivelser af følsomme personoplysninger til politiet som led i anmeldelsen af strafbart forhold. Der vil i den forbindelse kunne lægges vægt på, at de pågældende oplysninger vil skulle behandles af politiet med henblik på myndighedsudøvelse, jf. det anførte i betænkningens side 201 om bl.a. sociale myndigheders behandling og videregivelse af mistanke om incest til bl.a. politiet.

Oplysninger om strafbare forhold

Rigspolitiet har noteret sig, at den foreslåede regulering af behandling af *strafbare forhold* i al væsentlighed svarer til de gældende bestemmelser i persondataloven, samt at det fremgår af lovforslagets bemærkninger, at begrebet "strafbare forhold" antages at skulle forstås på tilsvarende måde som efter gældende ret.

Efter Rigspolitiets opfattelse kan det dog med fordel præciseres i bemærkningerne, at det ikke er enhver oplysning om et muligt strafbart forhold, herunder enhver anmeldelse til politiet, der kan anses for omfattet af begrebet, idet det forudsætter, at anmeldelsen til politiet i en eller anden form underbygges, førend der er tale om oplysninger om strafbare forhold, evt. med en henvisning til pkt. 3.10.2.2 i betænkningen.

Videreførelsen af gældende ret indebærer efter Rigspolitiets opfattelse, at *offentlige myndigheder* kan behandle oplysninger om strafbare forhold på baggrund af værdispringsreglen i lovforslagets § 8, stk. 2, nr. 2, eller på baggrund af en nærmere nødvendighedsvurdering, jf. § 8, stk. 2, nr. 3 og 4. Lovforslagets regler antages således at indebære, at offentlige myndigheder kan behandle, herunder videregive, oplysninger om strafbare forhold til politiet, f.eks. som led i myndighedens tilsyns- og kontrolopgaver og i forbindelse med rådgivning af politi- og anklagemyndighed om f.eks. retspraksis mv. Tilsvarende antages det, at offentlige myndigheder har den fornævnte brede adgang til at videregive oplysninger om strafbare forhold til politiet i forbindelse med indgivelse af en politianmeldelse.

Det er Rigspolitiets opfattelse, at rammerne for *offentlige myndigheders* behandling, herunder videregivelse, af oplysninger om strafbare forhold til politiet bør præciseres i bemærkningerne til lovforslagets § 8, stk. 1 og stk. 2. Det bør således udtrykkeligt fremgå, at der kan videregives oplysninger om strafbare forhold til politiet med henvisning til, at hensynet til den offentlige interesse i at muliggøre strafforfølgning af forhold, der efter gældende ret er strafbelagt, må anses for at udgøre en interesse, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår, jf. § 8, stk. 2, nr. 2. Endvidere bør det fremgå, at videregivelse efter omstændighederne vil kunne være nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe, jf. § 8, stk. 2, nr. 3, eller nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige, jf. § 8, stk. 2, nr. 4.

For så vidt angår *privates* behandling af oplysninger om strafbare forhold bemærkes det, at det i bemærkningerne til lovforslagets § 8, stk. 3 og stk. 4, til dels er præciseret, at private kan registrere oplysninger om strafbare forhold med henblik på indgivelse af politianmeldelse, f.eks. om butikstyveri, og eventuel senere afgivelse af vidneforklaring i retten. Rigspolitiet skal anbefale, at der i relevant omfang ligeledes henvises til overvejelser svarende til de ovenfor anførte med henblik på at sikre, at der ikke i praksis opstår tvivl om, hvorvidt private nyder samme adgang til at videregive oplysninger til politiet som led i anmeldelser af strafbare forhold.

Generelle forhold

Som indikeret ovenfor bør det efter Rigspolitiets opfattelse også mere generelt fremgå af lovforslaget, at de generelle databeskyttelsesretlige principper, herunder

principperne om proportionalitet, saglighed og formålsbestemthed, må anses for efterlevet i forbindelse med en anmeldelse af strafbare forhold, idet en sådan videregivelse personoplysninger af såvel almindelig og følsom karakter, der ikke strider mod anden gældende ret, herunder f.eks. straffelovens § 165, må anses for at være saglig mv.

3. Oplysningspligt mv.

Efter Rigspolitiet opfattelse bør det fastsættes i lovforslaget, at de registreredes rettigheder efter databeskyttelsesforordningens artikel 12-15 og artikel 34 ikke finder anvendelse i forhold til behandling af personoplysninger, der kan afdække, at en anmeldelse af et strafbart forhold eller anden videregivelse af personoplysninger til kompetente retshåndhævende myndigheder til brug for retshåndhævelsesøjemed har fundet sted. Herved sikres det – inden for rammerne af databeskyttelsesforordningens artikel 23 – at afgørelsen af, om de pågældende rettigheder finder anvendelse, ikke vil bero på den enkelte dataansvarliges anvendelse af databeskyttelseslovens § 22, stk. 2, men at de pågældende videregivelser generelt er undtaget fra artikel 12-15.

Rigspolitiet tillægger det i denne forbindelse betydning, at politiet og de øvrige kompetente retshåndhævende myndigheder er de relevante til at vurdere om, og i givet i hvilken udstrækning, oplysninger om, at der er indgivet en anmeldelse af et strafbart forhold, kan videreformidles til den registrerede. Hensynet til at sikre de berørte registreredes rettigheder vil herefter finde sted som led i de kompetente retshåndhævende myndigheders anvendelse af retshåndhævelseslovens tilsvarende bestemmelser om oplysningspligt mv., der er udformet under hensyntagen til de særlige hensyn, der finder anvendelse på retshåndhævelsesområdet.

Særligt for så vidt angår behovet for at fastsætte undtagelse fra databeskyttelsesforordningens artikel 34 bemærkes det, at dette ligeledes bør finde sted i forhold til de tilfælde, hvor den dataansvarlige konkret vurderer, at der er belæg for at indgive anmeldelse af et strafbart forhold i anledning af et bud på persondatasikkerheden. Det kan eksempelvis være tilfælde i forbindelse med visse former for it-kriminalitet, hackerangreb mv., hvor efterforskningen konkret kan drage nytte af, at det endnu ikke er offentligt kendt, at den pågældende aktivitet er blevet afdækket. Med henblik på at begrænse omfanget af en sådan undtagelse – og tage behørigt hensyn til de registreredes interesse i at modtage underretning om et brud på persondatasikkerhed omfattet af bestemmelsen – kan undtagelsen begrænses i tid frem til det tidspunkt, hvor politiet konkret meddeler den dataansvarlige, at en underretning kan finde sted uden at kompromittere efterforskningen af det strafba-

re forhold. En sådan meddelelse forventes efter omstændighederne at kunne gives inden for forholdsvis kort tid.

4. Strafbestemmelser mv.

Det fremgår af lovforslagets bestemmelser om sanktioner i lovforslagets kapitel 12, at overtrædelse af databeskyttelsesforordningen, lovforslaget og regler udstedt i medfør af lovforslaget straffes med bøde eller fængsel indtil 6 måneder.

Strafferammerne i lovforslagets strafbestemmelser indebærer, at forældelsesfristen er 2 år, jf. straffelovens § 93. Efter straffelovens § 94, stk. 1, skal forældelsesfristen som udgangspunkt regnes fra den dag, da den strafbare virksomhed eller undladelse er ophørt.

Rigspolitiet skal hertil bemærke, at straffesager om overtrædelse af databeskyttelsesforordningen efter omstændighederne vil kunne antage en vis størrelse og kompleksitet. Hertil kommer, at efterforskningen af sager, der f.eks. først henvises til politiet efter at have været undergivet forudgående sagsbehandling hos tilsynsmyndigheden, eller som omfatter forhold, bevissikring mv. uden for dansk jurisdiktion må forventes at have en vis tidsmæssig udstrækning. I sådanne sager vil der være vanskeligt at gennemføre de nødvendige strafforfølgningsskridt med henblik på at afbryde sagens forældelse inden for to år. Rigspolitiet skal opfordre til, at dette spørgsmål overvejes nærmere.

Desuden indebærer strafferammen, at politiet begrænses i brugen af visse af retsplejelovens straffeprocessuelle tvangsindgreb og efterforskningsskridt i forbindelse med efterforskning af overtrædelser af bestemmelser i lovforslaget og i databeskyttelsesforordningen. Det bemærkes i den forbindelse, at i hvert fald sager, hvor de ganske betydelige bødestraffe, som databeskyttelsesforordningen hjemler, skal bringes i anvendelse, næppe i alle tilfælde vil kunne efterforskes uden brug af visse tvangsmidler, herunder indgreb i meddelelseshemmeligheden. Det kan i den forbindelse overvejes, om der eksempelvis ved mere kvalificerede overtrædelser af databeskyttelsesforordningen bør være en adgang til at foretage indgreb i meddelelseshemmeligheden eventuelt svarende til bestemmelsen i retsplejelovens § 781, stk. 2.

5. Ressourcemæssige konsekvenser for dansk politi

Rigspolitiet har noteret, at lovforslaget ikke indeholder overvejelser om de eventuelle ressourcemæssige konsekvenser, som lovforslaget indebærer. Rigspolitiet

har endvidere noteret, at hovedparten af den strafferetlige håndhævelse af databeskyttelsesforordningens strafbestemmelser, skal varetages af politi- og anklagemyndigheden.

Rigspolitiet har ikke på det foreliggende grundlag kunnet foretage en nærmere vurdering af, hvilke ressourcemæssige konsekvenser den række af nye – til dels komplekse – strafferetlige delikter, der indføres i forhold til hele den private sektor og eventuelt hovedparten af den offentlige sektor, vil kunne give anledning til. Rigspolitiet skal derfor opfordre til, at Justitsministeriet nærmere overvejer omfanget af det forventede ressourcetræk for politiet i den forbindelse, og skal anmode om at blive inddraget i en sådan eventuel proces.

Med venlig hilsen

Helle Stigaard Jensen
sektionsleder

Justitsministeriet - databeskyttelseskontoret
databeskyttelse@jm.dk

Dato: 22. august 2017

Høring over udkast til databeskyttelsesloven

Ringsted Kommune
Koncerncenter

Sct. Bendtsgade 1
4100 Ringsted

Dir.: +45 57 62 60 23
Mail.: KRLS@RINGSTED.DK

koncerncenter@ringsted.dk
www.ringsted.dk
CVR-nr.: 18957981

Åbningstid:
Man.-Torsdag 11-15
Fredag 11-13
Telefontid:
Man.-Torsdag 10-15
Fredag 10-13

Justitsministeriet har ved mail af 28. juli 2017 anmodet om Ringsted Kommunes bemærkninger til udkast til forslag til databeskyttelseslov. Ringsted Kommune takker for henvendelsen og skal i den forbindelse fremkommen med nedenstående bemærkninger:

Generelt:

- Ringsted Kommune finder det uhensigtsmæssigt at kalde loven for databeskyttelsesloven, når den hovedsaglig omhandler og er rettet mod, personhenførbare data og ikke data i al almindelighed. Ringsted Kommune finder, at "persondataloven" er en mere retvisende betegnelse og henstiller at derfor at den betegnelse fastholdes.
- I praksis er det ikke hensigtsmæssigt, at man både skal læse forordningen og loven. Det vil desuden også være en ny praksis for langt de fleste kommunale sagsbehandlere. Når præamplen derfor giver mulighed for at indarbejde elementer af forordningen, i det omfang det er nødvendigt af hensyn til sammenhængen og for at gøre de nationale bestemmelser forståelige, vil Ringsted Kommune foreslå, at der sker en større indarbejdelse, af de væsentligste elementer og de elementer som kommunale sagsbehandlere erfaringsmæssigt oftest anvender. Der tænkes her særlig på *kategorierne af oplysninger og betingelserne for at behandle dem*. Derudover kunne man måske gøre mere for at binde loven sammen. I forhold til de elementer fra forordningen som man har valgt at skrive ind i loven, kommer den til at virke lidt usammenhængende.
- Lovforslaget indeholder så mange bemyndigelser i forhold til udarbejdelse af bekendtgørelser, at loven ikke giver et samlet billede af den nationale regulering. Det er efter Ringsted Kommunes opfattelse uhensigtsmæssigt blandt andet fordi det gør det vanskeligt at operere med i praksis.

Bemærkninger til de enkelte bestemmelser:

- **§ 1, stk. 2:** Lovforslaget ændrer terminologien fra elektronisk til automatisk. Der synes ikke at være tiltænkt nogen realitetsændring. Det fremgår af bemærkningerne til lovforslaget, at begrebet ”automatisk databehandling” er sammenfaldende med ”edb” eller ”elektronisk behandling”. Det er Ringsted Kommunes opfattelse at elektronisk er mere sigende og et mere almindeligt anvendt og velkendt begreb, hvorimod en ændring til ”automatisk” vil kunne føre til fortolknings tvivl. Ringsted Kommune henstiller derfor at begrebet ”elektronisk” fastholdes.
- **§ 2, stk. 5**: Ringsted Kommune er af den opfattelse, at den nuværende praksis bør fastholdes. Det er ikke hensigtsmæssigt at indføre en 10 års grænse og det vil ikke gøre det lettere at administrere. Man vil fortsat skulle forholde sig til, hvorvidt oplysninger om afdøde kan behandles særlig i forhold til videregivelse, hvor man bl.a. vil skulle forholde sig til forvaltningslovens regler om tavshedspligt, arkivloven og sundhedsloven. Derudover kan der sagtens være et beskyttelseshensyn også 10 år efter en person er død. Der ses ikke at være nogen saglig grund til at ophæve denne beskyttelse.
- **§ 5, stk. 1:** I bestemmelsen er ”saglige formål” erstattet af ”legitime formål”. Det er uhensigtsmæssigt, da man i store dele af den offentlige forvaltning netop opererer med begrebet ”saglige formål”. Hvis noget er sagligt er det også legitimt, så hvis der ikke er tiltænkt nogen realitetsændring, henstiller Ringsted Kommune at ”saglig” erstatter ”legitim”. En ændring vil kunne føre til fortolkningstvivl og en større ensartethed i terminologien i lovgivningen gør den lettere for ikke-jurister at arbejde med og forholde sig til.
- **§ 5, stk. 2**: Eksemplerne i litra 1-5 hilses velkomne.
- **§ 6, stk. 2:** Ringsted Kommune er af den opfattelse, at der ikke bør indføres flere forskellige aldersgrænser, men at nye aldersgrænser bør lægge sig op ad eksisterende for at skabe sammenhæng og ensartethed. I øvrigt henstiller Ringsted Kommune at aldersgrænsen på 16 år, som forordningen indfører, bør skrives direkte ind i den danske lov, da der er tale om en væsentlig nyskabelse og da det vil give en bedre sammenhæng i loven.
- **§ 6, stk. 3** Det vil være hensigtsmæssigt, hvis der eksplicit tages stilling til om samtykke kræves fra en eller begge forældremyndighedsindehavere. I lovforslaget er angivet, at det er ”indehaver**en”**, som skal give samtykke, men da udgangspunktet er fælles forældremyndighed kan det give anledning til fortolkningstvivl. Derudover giver det i praksis ofte anledning til tvister.
- **§ 12, stk. 2** Se bemærkningerne til § 5, stk. 1 vedrørende ”legitim” og ”saglig”.
- **§ 40** Der bør henvises til dansk rets almindelige regler for at undgå tvivl om at de øvrige almindelige erstatningsbetingelser også være opfyldt.

- **§ 41, stk. 5** Ringsted Kommune finder det yderst uhensigtsmæssigt, at spørgsmålet om sanktioner i forhold til offentlige myndigheder endnu ikke er afklaret. Der er derudover behov for en afklaring af, om der er solidariske hæftelse for offentlige myndigheder og hvad det i givet fald kommer til at betyde for myndighederne.

Med venlig hilsen

Kristine Louise Schiøtt
Juridisk specialkonsulent

Ringsted Kommune
Koncerncenter
Juristteamet

RKU
Rektorkollegiet
for de Kunstneriske og
Kulturelle Uddannelser

Styrelsen for Forskning og Uddannelse
Uddannelses- og Forskningsministerie
att. fuldm. Marie Carlsen
e: mhc@ufm.dk;

2017-08-09
J.nr.:10/sags nr.
RKU/afsender
torben.holm@kadk.dk

Høringssvar: Forslag til lov om databeskyttelse

Rektorkollegiet for de Kunstneriske og Kulturelle Uddannelser (RKU) henviser til Forsknings- og Uddannelsesstyrelsens mail af 18. juli vedrørende høring om Forslag til lov om databeskyttelse.

RKU er opmærksom på den samlede indsats for at forbedre databeskyttelsen i Europa og kan derfor kun tilslutte sig:

- At der i regi af EU sker en sikring af borgernes personoplysninger og udveksling af disse, såvel i regi af offentlige institutioner som i private virksomheder i hele EU.

- At denne sikring, i form af EU's databeskyttelsesforordning, bliver udmøntet i separat dansk lovgivning. Det er vigtigt, at vilkårene for at administrere sikringen af personoplysninger i relation til øvrig dansk lovgivning er præcis, konkret og relevant. Dette har selvsagt også direkte betydning for RKU-institutionernes administration af lovgrundlag, interne regler og administrativ praksis.

- At udmøntningen af databeskyttelsesforordningen i lovforslaget i vidt omfang viderefører gældende regler. RKU påskønner således, at det vigtige hensyn til forbedret beskyttelse af personoplysninger ikke ser ud til at medføre omfattende ændringer af andet lovgrundlag eller af vores administrative praksis.

RKU har noteret sig, at databeskyttelsesforordningen, ligesom persondataloven, omfatter *al it-behandling af personoplysninger* (på nær myndigheders brug af oplysninger til varetagelse af statens sikkerhed). RKU lægger derfor vægt på, at udmøntningen af loven *ikke* medfører en administrative praksis på institutionerne, der ikke står i forhold til hensynet om bedre beskyttelse af persondata:

- Lovforslaget giver registrerede personer adgang til at gøre indsigelse om brug af data, ret til at få slettet data og ret til at begrænse behandlingen af data. Det er vanskeligt på forhånd at vurdere, om brugen af disse rettigheder vil udvikle sig til at medføre administrative opgaver, som de enkelte institutioner *ikke* oplever som rationelle.

- På de kunstneriske videregående uddannelser er brugen af cpr.nr. især knyttet til aftaler om ansættelse af medarbejdere m.v. Oplysninger om den enkelte studerende sker (som bekendt) ud fra et 6-cifret studienummer (STADS). Den enkelte studerende har her selv e-adgang til sine oplysninger. Det er derfor RKU's forventning, at loven ikke vil medføre en øget indsigelse fra ansatte eller fra studerende.

Eksempler på samspil mellem loven og administrativ praksis:

- Oplysninger om individuelle forhold for den enkelte studerende – som f.eks. sygeorlov – er i dag registreret i sammenhæng med den studerendes cpr.nr. Disse oplysninger er hidtil blevet journaliseret efter gældende regler. I medfør af lovforslaget vil sletning af personlige oplysninger som disse inden journalisering kræve, at institutionerne her ændrer procedurer.

- Danmarks Statistik udarbejder årligt data til RKU over udviklingen i kandidaternes beskæftigelse. Dette sker ud fra anonymiserede lister over kandidaternes cpr.nr. RKU offentliggør ale-

ne analyse af disse data på institutionsniveau. Det er RKU's forståelse, at denne praksis falder ind under lovforslagets § 10 og derfor ikke blive påvirket.

Lovforslaget fastsætter i § 41 rammer for straf til offentlige myndigheder ved overtrædelse af loven. Formodningen er for, at statslige institutioner følger påbud fra tilsynsmyndigheder. RKU gør derfor blot for god ordens skyld opmærksom på følgende som et emne, som - meningsfuldt - kun kan håndteres på nationalt niveau:

Persondataforordningens fastsætter i Artikel 83 (forslagets side 139) de generelle betingelser for at pålægge administrative bøder – på op mod 20 mio. EUR ved overtrædelse af bestemmelserne. Der henvises hertil i § 41, men der er eksplicit ikke taget stilling til muligheden for at pålægge straf til offentlige myndigheder (eller størrelsen af dem) (stk. 5). Forslaget går på at henstille til, at offentlige myndigheder ikke underlægges den bøderamme, der fremgår af EU's persondataforordning.

§ 41. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 6 måneder overtrædelse af:
Stk. 4. databeskyttelsesforordningens artikel 83, stk. 2, skal følges ved pålægges af straf efter stk. 1-3.
Stk. 5. [stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder udestår]

RKU har herudover ingen bemærkninger til bestemmelser vedr. national sikkerhed, vilkårene for private virksomheder, vilkår for data om børn, eller om afdøde personer.

Med venlig hilsen

Torben Holm
Sekretariatschef

Roskilde Universitet
Administration

Uddannelses og Forskningsministeriet
ATT: Marie Carlsen
mhc@ufm.dk

Ang. Høring om databeskyttelsesloven

DATO/REFERENCE	JOURNALNUMMER	DERES REFERENCE / JOURNALNUMMER
10.08.2017	2012-240	

ATT: Marie Carlsen

Hermed følger Roskilde Universitets bemærkninger til udkastet til forslag til databeskyttelsesloven.

1. Generelle bemærkninger:

Henset til forordningens meget omfattende og ressourcekrævende krav til dataindsamlende organisationer, herunder både tekniske og organisatoriske, finder Roskilde Universitet anledning til at fremsætte en generel bemærkning om den betragtelige byrde, som forordningen bliver for universiteterne i en tid med reducerede bevillinger, samt økonomiske og personalemæssige nedskæringer, og at vi i den sammenhæng henstiller til, at der bliver set nærmere på byrdernes omfang, og de økonomiske konsekvenser, med henblik på stillingtagen til kompensation herfor.

2. § 10, stk. 4

Roskilde Universitet henstiller til, at en evt. fastsættelse af regler efter forhandling ml. sundhedsministeren og justitsministeren tydeliggør om de påtænkte oplysninger i så fald skal kommunikeres til datasubjektets egen læge, eller hvilken anden sundhedsperson/organisation der vil være tale om.

Med venlig hilsen

Mads Tolderlund
Informationssikkerhedskonsulent
Telefon:+4546743086

RUC IT
Roskilde Universitet
Universitetsvej 2, Bygning 14.1
4000 Roskilde
www.ruc.dk/om-universitetet/organisation/administration/

Rådet for Digital Sikkerhed

18. august 2017

Rådet for Digital Sikkerheds høringssvar til forslag til databeskyttelsesloven

Rådet for Digital Sikkerhed, RfDS, skal hermed takke for muligheden for at afgive høringssvar til "udkast til forslag til databeskyttelsesloven", DBL. RfDS benytter sig af lejligheden til samtidig at komme med enkelte bemærkninger til betænkning 1565, da betænkningen udgør et væsentligt fortolkningsbidrag til at forstå formuleringen af databeskyttelsesloven.

1. Overordnede bemærkninger

Ros til JM for et grundigt arbejde

RfDS vil indledningsvis takke Justitsministeriet, JM, for betænkning 1565. Betænkningen er et stort og grundigt arbejde, som er lavet på relativt kort tid henset til omfanget. Betænkningens format er, med dens opsummering af gældende ret, sammenligning med forordningens regler og mange steder gennemgang af relateret praksis og retspraksis, et værk som er yderst anvendeligt til en forståelse af persondataretten i en dansk kontekst. Betænkningen kan anvendes som opslagsværk for de fagpersoner, som skal beskæftige med området mange år fremover.

RfDS siger hermed mange tak til JM for en grundig og nyttig betænkning.

Glæde over de kommende vejledninger

RfDS noterer sig samtidig, at JM er klar over, at betænkningen ikke kan stå alene. På trods af dens kvalitet vil den næppe få en bred læserskare henset til dens omfang. Derfor noterer RfDS sig med glæde, at der også er planlagt en serie af vejledninger, som kortfattet og populært skal opsummere en række af betænkningen og databeskyttelseslovens regler, så de bliver tilgængelige for borgere, virksomheder og organisationer.

RfDS skal hermed udtrykke tilfredshed med, at der udarbejdes en serie kortfattede vejledninger om DBL og den praksis, den medfører.

Ændringer i gældende ret skal understreges og fortolkes harmoniseret

RfDS noterer sig, at JM gennem arbejdet med såvel betænkningen som databeskyttelsesloven har analyseret persondataforordningen således, at så store dele af gældende dansk ret kunne opretholdes som overhovedet muligt. RfDS er ikke begejstret for denne tilgang, da vi gerne så, at reglerne på det persondataretlige område overordnet bliver så harmoniserede som muligt indenfor EU. Det synes således at have været JMs ønske at nå den konklusion, at der ikke er tale om en ændring af gældende ret på trods af, at der i en række tilfælde er tale om, at der i lovgivningen inkluderes helt nye begreber. I de detaljerede bemærkninger nedenfor vil RfDS påpege et par eksempler på dette, f.eks. mht. konsekvensanalyser og databeskyttelse gennem design. I nær tilknytning hertil er det RfDS håb, at de kommende vejledninger tæt vil reflektere de vejledninger, der kommer fra artikel 29-gruppen, således at der ikke er risiko for, at det fremstår som om, at der er forskellig fortolkningspraksis mellem JM og artikel 29-gruppen.

RfDS håber, at man i det fremadrettede arbejde i høj grad vil skele til andre europæiske vejledninger på det persondataretlige område – herunder særligt fra artikel 29-gruppen – således at reglerne bliver så harmoniserede som muligt indenfor EU.

Der ligger et stort arbejde foran danske virksomheder og organisationer

RfDS noterer sig ligeledes, at JM i såvel betænkningen som i den kommunikation der har været om forordningen, betænkningen og databeskyttelsesloven understreger, at forordningen alene giver anledning til mindre justeringer af gældende ret og at det derfor for virksomheder og organisationer, som efterlever de eksisterende regler, ikke er en stor opgave at efterleve de nye regler. JM når frem til denne konklusion ved snævert at sammenligne de eksisterende regler med de fremtidige regler. RfDS kan ikke genkende dette billede. For det første er der i lovgivningen en introduktion af en række nye begreber og tilknyttede bestemmelser, som skal efterleves, jf. ovenfor. For det andet er der givetvis ganske mange virksomheder og organisationer, som ikke efterlever de eksisterende regler. Dette store flertal af virksomheder og organisationer vil opleve nødvendigheden af at efterleve gamle såvel som nye regler som en ganske stor arbejdsopgave. Når man sammenligner virkeligheden med de kommende regler, skal der gøres en betydelig indsats for at efterleve reglerne. For de projektledere, DPO'er, CPO'er m.v. som sidder med opgaverne bliver det ikke lettere at få ressourcer til arbejdet, når JM i sin kommunikation underdriver arbejdets omfang. For det tredje udestår der fortsat en lang række spørgsmål, når juraen skal anvendes på konkrete omstændigheder i den virkelige verden - ikke mindst fordi denne lovgivning i meget høj grad lægger op til et konkret skøn af forskellige forhold og tillige på mange områder er baseret på en retspraksis, som man ikke kan læse sig til direkte i lovgivningen. Det er skøn, som det er vanskeligt at foretage for virksomheder og organisationer, som ikke har en ekspert tilknyttet og som ikke har et budgetmæssigt rum til at få det.

RfDS skal opfordre til, at JM i sin kommunikation ikke nedtoner forbedringerne i de nye regler eller tager let på de udfordringer, som virksomheder og organisationer står overfor, når de skal til at efterleve de nye regler.

Styrkelse af Datatilsynet

RfDS noterer sig yderligere, at JM i betænkning 1565 i afsnit 7.5.4 ikke i fornødent omfang understreger det store merarbejde, som forordningen vil betyde for Datatilsynet. Hermed er der en risiko for, at der ikke fra politisk side er den fornødne opmærksom på at styrke Datatilsynet tilstrækkeligt. Når man sammenligner de opgaver, der pålægges Datatilsynet i direktiv 95/46/EF, artikel 28 med beskrivelsen i forordningens artikel 57 kan man konstatere, at der er tale om et meget betydeligt øget omfang af arbejdsopgaver. Der er i praksis kun få arbejdsopgaver der ændres, og endnu færre der falder bort. Det ligger RfDS meget på sinde, at især artikel 57, stk. 1, litra b, d og i, som omhandler den viden om reglerne, som Tilsynet pålægges at bibringe omverdenen, bliver på et tilfredsstillende niveau. Desuden er det vigtigt, at der er fokus på den EU-harmonisering, som forordningen trods alt stadig giver mulighed for, og som er defineret som Tilsynets arbejdsopgaver og især adresseres i artikel 57, litra g, h og t. RfDS mener, at vi har brug for et Datatilsyn, som ikke kun er Tilsyn, men også i høj grad kan informere konkret om reglernes anvendelse, når der er brug for det. Et tilsyn som kan agere proaktivt, har ressourcer til at tage sager op af egen drift, har moderne kommunikationsfaciliteter, er involveret i den offentlige debat, tager stilling til konkret anvendelse af nyere teknologier, har en åbningstid der svarer til omverdenen, fungerer som et nationalt kompetencecenter for persondatabeskyttelse (gerne med tilknytning til såvel den juridiske som den tekniske forskningsverden) og som tilvejebringer vejledninger og redskaber til at understøtte offentlige og private organisationers implementering af forordningens regler.

RfDS vil derfor med dette høringssvar appellere til en markant styrkelse af Datatilsynet.

Udnyttelse af nationale særregler

Rådet noterer sig, at JM generelt har udnyttet mange af forordningens muligheder for at fastsætte national lovgivning. Rådet skal bemærke, at når disse muligheder udnyttes, så undermineres et af hovedformålene med forordningen; nemlig at skabe harmonisering i EU. Borgernes data vil blive behandlet forskelligt i de forskellige EU-lande. Virksomhederne i deres roller som dataansvarlige og databehandlere får øgede omkostninger, når de, for så vidt angår de områder hvor der udnyttes muligheder for at fastsætte national lovgivning, skal tilpasse deres it-systemer og procedurer til 28 forskellige nationale regelsæt. De nationale særregler vil være en hæmsko specielt for SMV'erne i forhold til at få adgang til det indre marked.

RfDS skal henstille til, at der fra politisk side tages hensyn til det indre markeds målsætninger om fri bevægelighed således at der kun anvendes national lovgivning, hvor det skønnes absolut nødvendigt.

2. Detaljerede bemærkninger til DBL

Krigsreglen

RfDS har noteret sig, at der er lagt op til en ændring af krigsreglen fra PDL § 41, stk. 4. Ændringen jf. DBL § 3, stk. 9 betyder, at man går fra at kunne bortskaffe personoplysninger i tilfælde af krig til at vurdere om personoplysninger i nærmere bestemte IT-systemer, må placeres i udlandet. Det bagvedliggende hensyn præciseres samtidig p. 259 til ikke at være IT-sikkerhed, men alene at være statens sikkerhed. På den måde må det forventes, at der bliver tale om en klart afgrænset og gennemsigtig liste af konkrete systemer, som ikke må placeres udenfor landets grænser. RfDS er meget tilfredse med denne modernisering og præcisering af krigsreglen, som implicit anerkender, at hvis IT-sikkerheden er på plads, så betyder det ikke noget, hvor i EU personoplysningerne er placeret.

RfDS er tilfreds med ændringen af krigsreglen men skal opfordre til, at der anlægges snævre betragtninger baseret på risikovurderinger af, hvilke IT-systemer, som kan omfattes af hensynet til statens sikkerhed.

Offentlige myndigheder kan viderebehandle til andre formål med undtagelser for oplysningspligten

RfDS er skeptiske overfor, at offentlige myndigheder jf. DBL § 5, stk. 3 kan få fastsat regler, der sikrer viderebehandling af personoplysninger til andre formål, end de oprindeligt var indsamlet til, uafhængigt af formålenes forenelighed. RfDS finder for det første, at bestemmelsen er meget bred. Når først en offentlig myndighed er kommet i besiddelse af en personoplysning, kan den principielt set ende hvor som helst og anvendes til et hvilket som helst formål (selvfølgelig forudsat at der er en regel). Når denne bestemmelse så ses i sammenhæng med DBL § 23 og § 22, stk. 2 og 3 om undtagelserne i oplysningspligten og indsigtsretten, som betyder, at det bliver grænsende til umuligt for de registrerede at benytte rettighederne i artikel 16, 17, 18 og 21, betyder det, at DBL medvirker til at sikre en fuldstændig uigennemsigtighed for borgerne om, til hvilke formål og af hvilke myndigheder deres personoplysninger behandles. Tilsvarende gælder for behandling i videnskabeligt øjemed, jf. DBL § 22, stk. 5.

Det klæder ikke et demokratisk samfund at have sådanne regler. Det bør reducere tilliden til den offentlige sektors behandling af personoplysninger og formodentlig også til den offentlige sektors digitalisering.

Argumenterne for at den offentlige sektor skal have disse regler anføres bl.a. effektivitet (p. 168) og byrder (p.210). Der synes ikke at være tilsvarende betragtninger om, at der er byrdefuldt for de private virksomheder, som der ikke er tilsvarende undtagelser for, at efterleve reglerne. Der findes således en asymmetri i reglerne mellem den offentlige og private sektor.

Endelig finder RfDS, at man i hvert fald kan diskutere, om den undtagelsesbestemmelse, der er indsat i forordningens artikel 23, stk. 1, litra e om medlemsstaternes "væsentlige økonomiske eller finansielle interesser", og som JM anvender som retligt grundlag for undtagelserne, er tiltænkt denne anvendelse. Interesserne uddybes i litra e med "herunder valuta-, budget- og skatteanliggender". Man kan diskutere, om medlemsstaterne ikke alene bør anvende undtagelsesbestemmelsen snævert, når der er større forhold på spil, som f.eks. en væsentlig påvirkning af BNP, end at JM ønsker at købe billigere it-systemer og ønsker en billigere offentlig forvaltning. Hertil kommer at man kan diskutere om begrænsningen "respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i det demokratisk samfund", jf. artikel 23 stk. 1 og JMs egen formulering i § 22, stk. 2 om, at undtagelser kun bør anvendes, hvis der er "afgørende hensyn til offentlige interesser".

At sætte et de fundamentale principper fra forordningens artikel 5 ud af kraft samtidig med at man tilsidesætter nogle af de registreredes rettigheder i artikel 14 og 15, der gør det grænsende til umuligt for de registrerede at udnytte deres rettigheder fra artiklerne 16, 17, 18 og 21 og samtidig anvende en undtagelsesbestemmelse, som man i hvert fald kan diskutere om den ikke er tiltænkt vigtigere formål end de skitserede, synes stærkt betænkeligt.

JM anfører flere steder, at de nye regler ikke fører til en ændring af praksis, men tværtimod er fastsat for at opretholde eksisterende retspraksis, f.eks. p. 150. Uanset om der sker en ændring af praksis eller ej, synes det betænkeligt at have en praksis som skitseret ovenfor. Forordningen kunne anvendes som en anledning til at rette op på det, og give de registrerede en bedre beskyttelse.

RfDS skal opfordre til, at bestemmelsen i §5 stk. 3 fjernes således at alle myndigheder skal anvende §5, stk. 2 ved vurdering af, om to formål er forenelige. Desuden skal RfDS opfordre til, at bestemmelse i § 23 og § 22, stk. 2 anvendes langt mere snævert, end der er lagt op til, således at det kun er helt undtagelsesvist, at der er undtagelse for oplysningen om behandling. For så vidt angår DBL § 22, stk. 3 tager RfDS det til efterretning, at reglerne om indsigt efter DBL bringes i overensstemmelse med reglerne i forvaltningsloven.

De arbejdsretlige regler

DBL indeholder flere forskellige steder regler, som er af betydning for arbejdsretten, f.eks. DBL § 7, stk. 2 om følsomme oplysninger, § 8, stk. 3 og 4 om straffeoplysninger, herunder straffeattest og § 12 om generel behandling af personoplysninger på arbejdsmarkedet i medfør af lov og overenskomster. Særligt på det arbejdsretlige område fastslås det, at den offentlige forvaltning kan behandle oplysninger med interesseafvejning, selv dette i øvrigt generelt er udelukket den offentlige forvaltning. Det fastslås også, så der ikke er tvivl, at samtykke kan bruges som retligt grundlag for behandling af personoplysninger. RfDS

tager disse fortolkningsbidrag til efterretning, og vil gerne udtrykke tilfredshed med, at DBL sikrer, at der ikke skabes usikkerhed om reglernes anvendelsesområde på arbejdsmarkedet.

I det omfang en personoplysning via praksis har været klassificeret som en dansk PDL §8 oplysning om strafbare forhold, væsentlige sociale problemer og andre rent private forhold skal oplysningen reklassificeres som enten en almindelig eller en følsom oplysning, da de rent private oplysninger bortfalder med forordningen. Af artikel 10 om behandling af oplysninger om strafbare forhold fremgår det, at behandlingen kan foretages på baggrund af artikel 6 stk. 1, hvorfor oplysninger om strafbare forhold må anses for at være en art almindelig oplysning. Dette konkluderes også meget hurtigt i lovforslaget p. 174 og p. 187. Det er centralt at fastslå, at man ikke derfor kan konkludere, at alle PDL § 8 oplysninger automatisk bliver almindelige oplysninger under forordningen. I betænkningen findes i relation til artikel 88 en glimrende beskrivelse af det arbejdsretlige område herunder en beskrivelse af, hvilken klassifikation der gennem praksis er fastlagt. Det ville have været nyttigt, dersom JM i betænkningen havde taget stilling til en reklassifikation af de arbejdsretlige § 8 -oplysninger om rent private forhold. Personlighedstest, som hidtil har været en oplysning om rent private forhold kan f.eks. næppe passes ind i som en følsom oplysning efter artikel 7 og må derfor antages at være en almindelig oplysning efter artikel 6, hvorimod alkoholtest i form af blodprøver, som også hidtil har været en §8 oplysning om rent private forhold, formodentlig godt fremadrettet kan antages at være en helbredsoplysning og dermed en følsom oplysning efter artikel 9.

Da det arbejdsretlige område er af betydning for alle arbejdsgivere og lønmodtagere, skal RfDS hermed opfordre til, at der laves en særskilt vejledning eller udtalelse evt. fra Datatilsynet om reklassifikation af PDL § 8 oplysninger.

Sanktioner

RfDS har noteret sig, at der med § 42 er lagt op til, at Datatilsynet kan udstede bødeforlæg som nærmere omtalt p. 238 og p. 246. Såfremt bødeforlægget ikke accepteres, skal Datatilsynet foretage politianmeldelse med bl.a. indstilling om bødens størrelse. Desuden skal Datatilsynet jf. bemærkningerne p. 247 høres herunder om bødens størrelse førend der træffes afgørelse om tiltale spørgsmål.

RfDS vil gerne tilkendegive fuld støtte til at tildele Datatilsynet kompetencer, som angivet ovenfor, idet det på pragmatisk vis løser udfordringen med at udstede administrative bøder henset til begrænsningerne i Grundloven.

Videre noterer RfDS sig, at JM lægger op til at overtrædelsen af artikel 10 om oplysninger om strafbare forhold også skal strafsanktioneres i dansk ret. Det synes ganske rimeligt at strafsanktionere denne overtrædelse, ligesom det gør sig gældende for de øvrige almindelige og for de følsomme oplysninger.

RfDS kan derfor bakke op om, at der sanktioneres ved overtrædelse af artikel 10.

Endelig noterer RfDS sig, at der i JM udkast til DBL, jf. § 41, stk. 5 ikke er taget stilling til om offentlige myndigheder kan sanktioneres. RfDS finder, at det er rimeligt, at der introduceres bøder til den offentlige sektor. For det første har det en betydeligt større afskrækkende effekt at der kan trækkes penge ud af et budget til bøder end at der kan komme et brev fra Datatilsynet, hvori der udtales kritik. Bøder er med andre ord et meget stærkt incitament til at overholde loven. For det andet et det vigtigt for retfærdighedsopfattelsen i samfundet at der er lighed for loven. Den samme overtrædelse skal straffes ens

uanset om man er offentlig eller privat. For det tredje er det vigtigt, at der sker harmonisering i Europa. Danmark bør ikke være et discount land når det kommer til at straffe overtrædelser i den offentlige sektor. Når borgerne desuden skal være mobile jf. det indre marked, vil det forekomme besynderligt, hvis de lande de agerer i straffer de offentlige myndigheder forskelligt.

De fleste af argumenterne imod bøder til den offentlige sektor synes at kunne afvises. En offentlig myndighed, som får en bøde kan ikke reducere sine serviceforpligtelser, som typisk er lovbestemte – f.eks. plejehjem og børnehaver. Pengene skal hentes et andet sted – f.eks. på anlægsinvesteringer eller fra reserver. Et andet argument mod bøderne er at der sædvanligvis ikke udstedes bøder til det offentlige under henvisning til straffelovens § 27, stk. 2. Der findes dog adskillige eksempler på at den offentlige sektor alligevel kan modtage bøder – f.eks. på i forhold til arbejdsmiljølovgivningen, fødevarelovgivningen eller udbudsloven.

RfDS finder, at der skal ske en ligestilling mellem den offentlige og den private sektor, således at begge sektorer kan idømmes de samme bøder for de samme overtrædelser.

Brede rammer for regeringen til at lave nationale bestemmelser

RfDS noterer sig, at der med § 44 indføres ganske vide bestemmelser for både Justitsministeren og for andre ministre indenfor deres ressort at fastlægge særregler uden at disse skal forelægges Folketinget – ikke mindst jf. uddybningen pp. 321-322.

RfDS finder, at denne problemstilling er tæt relateret til den problemstilling, som fremgik af Kommissionens oprindelige udkast til forordning fra januar 2012, hvoraf det fremgik, at Kommissionen på en meget lang række områder kunne udstede delegerede retsakter, med det formål at sikre en stærk harmonisering af reglerne. Kommissionens ret til at fastsætte delegerende retsakter er under forhandlingerne om forordningen blevet væsentligt reduceret, bl.a. fordi man var bange for at det ville skabe uforudsigelighed i regeldannelsen, hvis man administrativt kunne fastsætte sådanne regler. Hvis alle medlemsstaterne benytter sig af tilsvarende muligheder for løbende at fastsætte regler efter behov får man den samme forudsigelighed bare på nationalt. Det er en endnu værre situation, fordi vi så med sikkerhed får 28 forskellige implementeringer og dermed en lige så fragmenteret lovgivning, som under det eksisterende direktiv 95/46/EF.

Rådet anser tiltag som § 44 for at kunne medvirke til en begrænsning af harmoniseringen af reglerne på det persondataretlige område og opfordrer til, at § 44 kan fjernes eller indskrænkes mest muligt.

3. Detaljerede bemærkninger til betænkningen

RfDS har foruden bemærkninger, der knytter sig til DBL, også en række andre bemærkninger vedrørende persondataretlige forhold. Da disse bemærkninger formodentlig ikke vil indgå i JMs overvejelser i relation til høring af loven, vil RfDS formodentlig rette en selvstændig og direkte henvendelse til Justitsministeren desangående.

Backup

RfDS anser det for en væsentlig praktisk udfordring, hvordan man i fremtiden skal indrette sine backupløsninger. Backup er en kopi af såvel data som it-systemer, der gemmes separeret fra de oprindelige data og it-systemer med henblik på at kunne bringes i anvendelse, hvis de oprindelige data eller it-systemer rammes af fejl, ondsindet kode som f.eks. ransomware eller tyveri i form af hacking og dermed ikke længere er tilgængelige eller har fået krænket fortrolighed eller integritet.

I sikkerhedsstandarden ISO/IEC 27002:2013 kontrol 12.3 fremgår det, at: "Der bør tages backupkopier af informationer, software og systembilleder, og disse bør testes regelmæssigt i overensstemmelse med den aftalte backuppolitik". Standarden skal efterleves af statslige myndigheder. I den seneste digitaliseringsstrategi er der en hensigt om at regioner og kommuner efterlever den. Desuden efterlever mange private virksomheder standarden. Backup er med andre ord et teknisk sikkerhedstiltag, som i mange år har været en følge af god sikkerhedsskik, sikkerhedsstandarder, og anbefalet af offentlige myndigheder.

Det følger af standarden m.v., at der etableres en backuppolitik, som skal testes. En række backupløsninger er baseret på princippet om, at de ikke kan ændres, fordi det i sig selv er en sikkerhedstrussel, hvis backupdatas eller -it-systemers integritet er udfordret: Hvis f.eks. en online harddisk backup kan ændres, kan den inficeres med ransomware samtidig med at produktionsdata og produktionssystemer inficeres, og så har organisationen ikke længere en backup.

Direktiv 95/46/EF, artikel 17, stk. 1, Lov om behandling af personoplysninger, § 41, stk. 3 og forordningens artikel 32, stk. 1 lægger op til, at dataansvarlige og databehandleren skal gennemføre "evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse" (litra c), hvilket i en række tilfælde kun kan ske ved at genindlæse en backup. Der er i medfør af lovgivningen med andre ord en pligt til at tage backup, da det er den eneste måde, man i forhold til en række konkrete sikkerhedsbrud vil kunne genoprette oplysningerne.

Den registreredes ret til sletning er fastslået i direktiv 95/46/EF, artikel 12, litra b, Lov om behandling af personoplysninger §37 og i forordningens artikel 17, hvor det i stk. 1 hedder: "Den registrerede har ret til at få personoplysninger om sig selv slettet af den dataansvarlige uden unødig forsinkelse, og den dataansvarlige har pligt til at slette personoplysninger uden unødig forsinkelse" under forudsætning af at et af flere forhold gør sig gældende. Retsstillingen mht. indsigt og sletning er med forordningen ikke ændret væsentligt.

RfDS finder, at der er en konflikt mellem på den ene side at tage backup og på den anden side at efterkomme en anmodning om sletning eller berigtigelse. Teknisk er det i en række sammenhænge umuligt at berigtige eller slette personoplysninger fra backup. Uanset at retsstillingen er uændret med forordningen, er det en udfordring, som aldrig er blevet løst. RfDS skal anmode om, at JM evt. med hjælp fra Digitaliseringsstyrelsen og Datatilsynet, supplerer sin liste over planlagte vejledninger med en vejledning om, hvordan man teknisk skal kunne efterleve dette krav.

Konsekvensanalyser

I betænkningen har JM gennemgået reglerne for, hvornår der skal udarbejdes konsekvensanalyser pp. 522-537. Reglerne er gennemgået helt således som de præsenteres i forordningen: der skal lægges vægt på om behandlingen udgør en høj risiko for de registrerede og de tre eksempler, der gives i forordningens artikel

35, stk. 3, på hvornår der skal gennemføres konsekvensanalyser, er gengivet. JM fastslår herefter, at der er tale om en udvidelse af gældende ret, og drager samtidig den konklusion baseret på eksemplerne og flere præambelbetragtninger, at "området for, hvornår en konsekvensanalyse er påkrævet er snævert. Dataansvarlige må således i de fleste tilfælde antages ikke at skulle udarbejde en konsekvensanalyse", p. 534.

JMs gennemgang af konsekvensanalyserne synes præget af at understrege at der for langt de fleste dataansvarlige ikke sker noget nyt med forordningen. RfDS finder, at JM's gennemgang på den ene side er ordentlig og saglig men på den anden side er overdrevet forsigtig i forhold til at stille nye krav. F.eks. har artikel 29-gruppen i wp 248, pp. 7-9 opstillet 10 kriterier for, hvornår virksomheder og organisationer skal overveje at gennemføre konsekvensanalyser. Disse kriterier synes at udvide anvendelsen af konsekvensanalyser ud over hvad der redegøres for af JM. Kriterierne blev vedtaget i april og har i øvrigt været kendt i udkast længe, altså et godt stykke tid inden udgivelsen af betænkningen.

RfDS vil gerne påpege, at området for anvendelsen af konsekvensanalyser synes lidt bredere, end det umiddelbart fremgår af betænkningen. RfDS vil samtidig påpege, at det er vigtigt, at rådgivningen fra offentlige myndigheder mht. de persondataretlige regler ikke er for forsigtig. Det er dyrt at skulle lave løsninger om, hvis kravene bliver fortolket mere skærpet end først antaget, end det er at lave løsningerne mere sikre fra starten.

Databeskyttelse gennem Design

Databeskyttelse gennem design, DPbD, kendes ikke som juridisk begreb fra hverken persondatadirektivet eller persondataloven. Det er et nyt begreb, som introduceres i persondataforordningens artikel 25. I Betænkningen konkluderer Justitsministeriet imidlertid, at området er "dækket af flere bestemmelser i gældende ret", p.410, og at "Databeskyttelsesforordningens artikel 25 etablerer ikke i sig selv nye krav til den dataansvarlige", p. 422. RfDS er uenig i den udlægning af forordningen. RfDS finder, at JM også på dette område er for forsigtige med at bruge forordningen til at tolke et nyt indhold ind i persondataretten.

JM fastslår herefter, at artikel 25 stiller krav til, at der skal gennemføres passende tekniske og organisatoriske foranstaltninger både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen. Det fastslås af JM, at det er nyt, at foranstaltningerne skal fastlægges på tidspunktet for fastlæggelse af midlerne. RfDS er enig i denne betragtning.

RfDS mener, at artikel 25 stiller nye krav til de dataansvarlige. Når JM når frem til deres konklusion skyldes det formodentlig, at JM finder, at der er overensstemmelse mellem de passende tekniske og organisatoriske foranstaltninger, der stilles efter artikel 25 og artikel 32. RfDS finder derimod, at der er tale om to typer af foranstaltninger, hvorefter den ene type kan siges at være designkrav, mens den anden type kan siges at være sikkerhedskrav. På visse punkter er der et overlap mellem de to typer af foranstaltninger forstået således, at en given foranstaltning godt kan være både designmæssig og sikkerhedsmæssigt begrundet, f.eks. pseudonymisering. RfDS mener derfor, at JM overser et selvstændigt materielt indhold i artikel 25.

I artikel 32 stilles der krav om foranstaltninger, der skal passe til de risici den teknologiske løsning indebærer. Der nævnes eksempler på teknologier i form af pseudonymisering og kryptering, der nævnes målsætninger som tilgængelighed, fortrolighed, integritet og robusthed og der nævnes organisatoriske tiltag som tests. Listen kan siges at være uddybet i sikkerhedsbekendtgørelsen, hvor der nævnes konkrete tiltag som logning, adgangskontrol og fysisk sikkerhed. Sikkerhedsbekendtgørelsen falder imidlertid bort med

forordningen og afløses af en konkret risikovurdering af hvilke foranstaltninger, der er behov for. I artikel 32 gives der altså eksempler på hvad sikkerhed er, men der stilles ikke eksplicitte krav til hvilke foranstaltninger, der skal iværksættes. Den dataansvarlige skal selv vurdere hvilket materielt indhold, der ligger i bestemmelsen ud fra sine konkrete behandlinger, risici, m.v.

Tilsvarende i artikel 25, hvor der som eksempler på teknologier nævnes pseudonymisering og som målsætninger nævnes dataminimering, andre databeskyttelsesprincipper og tilgængelighed. Artikel 25 giver altså også eksempler på, hvad der skal forstås ved design, men der stilles ikke eksplicitte krav til hvilke foranstaltninger, der skal iværksættes. RfDS mener, at også her skal den dataansvarlige selv vurdere hvilket materielt indhold, der ligger i bestemmelsen ud fra sine konkrete behandlinger, risici, m.v.

Til støtte for dette synspunkt kan det konstateres, at begrebet passende tekniske og organisatoriske foranstaltninger anvendes flere steder i forordningen. Det er imidlertid ikke givet, at betydningen af ordvalget er den samme i alle situationer. F.eks. i artikel 28, stk. 3 litra e er de foranstaltninger der skal iværksættes nogle, som skal hjælpe databehandleren med at opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger fra de registrerede. Disse foranstaltninger er ikke overlappende med sikkerhedsforanstaltningerne i artikel 32. Et andet eksempel kan findes i artikel 24, stk. 1 hvor foranstaltninger har til formål at være i stand til at påvise, at behandling er i overensstemmelse med forordningen. Også disse foranstaltninger må siges at være nogle andre end sikkerhedsforanstaltningerne fra artikel 32.

Hvad ligger der så i tekniske og organisatoriske foranstaltninger, som kan understøtte databeskyttelse gennem design? Begrebet privacy by design stammer fra Ann Cavoukian, som i 90'erne opstillede syv principper, der skulle bruges som guideline, når der blev designet it-systemer, der skulle behandle personoplysninger. Disse principper blev vedtaget i en resolution på Datatilsynenes 32 internationale konference i 2010 og det danske Datatilsyn henviser til dem:

- Proaktiv, ikke reaktiv
- Privacy som standardindstilling
- Privacy skal være indlejret I systemet
- Der skal være fuld funktionalitet
- Beskyttelse i hele livscyklussen
- Synlighed og trasparens
- Brugeren i centrum

Princip nummer tre giver en god indikation af, at lovgiver har tænkt på disse principper i og med at dette er integreret direkte i artikel 25, stk. 2. Som det fremgår, er disse principper ikke nødvendigvis sikkerhedsforanstaltninger med i stedet designforanstaltninger. Det er f.eks. ikke en sikkerhedsforanstaltning at indlejre noget i en teknologi. Det er en designforanstaltning.

Ud over Ann Cavoukians principper findes der flere andre sammenstillinger af designprincipper, som man kunne tage udgangspunkt i for at kortlægge det selvstændige materielle indhold i DPbD, f.eks. Hoepmans designstrategier, som ENISA har taget udgangspunkt i en rapport, eller Borking and Blarkom om privatlivsfremmende teknologier, som understøtter både/eller sikkerhed og design. Det vil imidlertid være for omfattende at berøre alle disse tilgange i dette høringssvar. Cavoukians principper er imidlertid

tilstrækkeligt til at illustrere at DPbD har et materielt selvstændigt indhold, der er forskelligt fra sikkerhedsforanstaltninger.
JM anfører, at artikel 29-gruppen i flere udtalelser har stillet krav om designforanstaltninger. Som eksempel har artikel 29-gruppen i Opinion 01/2015 om privacy i droner netop opfordret til: "Embed privacy friendly design choices and privacy friendly defaults as part of a privacy by design approach". Alle de udtalelser, som involverer noget om design, er så vidt vides fra efter januar 2012, hvor første udkast til forordningen blev offentliggjort, og i hvert fald efter princippet blev skabt af Cavoukian i 90'erne. Man kan sige, at artikel 29-gruppen med udtalelsen har taget forskud på glæderne ved artikel 25 inden den fik virkning.

Pointen er ikke en lang juridisk akademisk diskussion af, om hvorvidt en given passende teknisk eller organisatorisk foranstaltning er en designforanstaltning eller en sikkerhedsforanstaltning. Pointen er, at hvis designforanstaltninger ikke i sig selv tillægges et materielt indhold, overser man alle de foranstaltninger, som kan siges alene at være designmæssige, og dermed at have deres retlige grundlag i artikel 25 uden at være sikkerhedsmæssige med retligt grundlag i artikel 32. Man bruger så at sige kun halvdelen af værktøjerne i værktøjskassen. Hvis der derimod tillægges et selvstændigt materielt indhold til DPbD, skabes der en passende teknisk og organisatorisk understøttelse af f.eks. dataklassifikation, dataportabilitet og oplysningspligt.

RfDS finder, at JM har overset, at der ligger et materielt indhold i artikel 25, som defineres af de brede mængde af muligheder, der er for at designe beskyttelse af personoplysninger ind i sine løsninger. Hvilke designmæssige foranstaltninger der konkret skal iværksættes, afhænger ligesom foranstaltningerne i artikel 32 af de konkrete behandlinger m.v. Men artikel 25 indebærer en pligt til at overveje et mulighedsrum af designmæssige foranstaltninger som ligger ud over, hvad der kan ske i medfør af artikel 32. Mulighedsrummet fastlægges ligesom for artikel 32 af konkrete vurderinger og af praksis. Ann Cavoukians principper er en del af dette designmæssige mulighedsrum. De designmæssige foranstaltninger kan bl.a. tilføjes til værktøjskassen omtalt i høringsudkastet pp. 184-185.

Rådet står naturligvis til rådighed for en uddybelse af ovenstående bemærkninger.

Med venlig hilsen

Bestyrelsen
Rådet for Digital Sikkerhed

RÅDET FOR ETNISKE MINORITETER

Til Justitsministeriet

HØRINGSSVAR

Dato:	22. august 2017
Kontor:	Sekretariatet
Sagsbeh.:	MNS

Høringssvar vedr. udkast til forslag til databeskyttelseslov

Hermed fremsender Rådet for Etniske Minoriteter svar på ovenstående høring.

Rådet for Etniske Minoriteter har ingen bemærkninger til den fremsendte redegørelse.

Med venlig hilsen

Yasar Cakmak

Formand for Rådet for Etniske Minoriteter

Sekretariatet for Rådet for Etniske Minoriteter
Strandgade 25C
1401 København K

Telefon: 72 14 28 32
Mail: rem@siri.dk
Web: www.rem.dk

SAMSØ KOMMUNE
www.samsoe.dk

Justitsministeriet

Databeskyttelseskontoret

databeskyttelseskontoret@jm.dk

16. august 2017

Sagsnr. 741-2017-3452
Dok.nr. 741-2017-18858
Journalnr.

Samsø Kommune
Søtofte 10, Tranebjerg
8305 Samsø

Telefon +45 8792 2200
Fax +45 8792 1128
E-mail: kommune@samsoe.dk

Ekspeditionstid
Mandag-torsdag 10.00 - 12.00
Torsdag tillige 15.00 - 17.00

Fredag lukket for ekspedition

Telefontid
Mandag-torsdag 09.00 - 12.00
13.00 - 15.00

Fredag er telefonen lukket

CVR/SE-nr. 23795515
EAN-nr. 5798006123971

Høringssvar fra Samsø Kommune over udkast til forslag til databeskyttelsesloven (2016-7910-0021)

Samsø Kommune finder, at lovforslaget i sin nuværende form forekommer (unødigt) omfattende og kompliceret.
Samsø Kommune vil derfor opfordre til, at ministeriet snarest muligt efter en evt. vedtagelse af loven udsender en overskuelig og gennemarbejdet vejledning, som kan fremme omsætningen af lovgivningen.

Med venlig hilsen

Marcel Meijer
Borgmester

Mogens Wehrs
Kommunaldirektør

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

Indledningsvis skal det bemærkes, at SikkerhedsBranchen hilser databeskyttelsesforordningens og særligt databeskyttelseslovens videreførelse af den gældende retstilstand med endnu flere rettigheder til de registrerede, skærpede krav til den dataansvarlige/databehandleren samt skærpede sanktioner velkommen.

De eneste bemærkninger vi har vedrører tv-overvågning, der jo eksplicit er omfattet af forordning og lov. Vi hilser meget velkomment, når der på side 323 i bemærkningerne til loven lægges op til, at kapitel 6a i den gældende persondatalov videreføres i lov om tv-overvågning. Det er blot vigtigt for os at understrege, at skulle det ikke ske er vi efterladt uden specifikke bestemmelser for tv-overvågning, hvilket vil være meget skadeligt.

Vi vil foreslå at man i lov om tv-overvågning indfører bestemmelser svarende til Straffelovens §§ 263 og 264 a, c og d. På den måde vil man have samlet de vigtigste bestemmelser om tv-overvågning i en lov. Som det er i dag, hvor bestemmelserne er spredt på tre love, er det meget vanskeligt for de dataansvarlige at danne sig et overblik over hvad man må og ikke må i sammenhæng med Persondatalovens generelle bestemmelser.

En bekymring, som fylder meget i branchen i relation til tv-overvågning, er den registreredes ret til indsigt. Som vi forstår det, er der i dag en ret for mennesker som er blevet registreret på tv-overvågning til at få indsigt i hvad der er registreret. Det vil sige se eller få billederne af sig selv.

Der er på den måde ikke meget nyt i forordningen. Det nye er den utrolige interesse, der er i samfundet og erhvervslivet for forordningen, og hvad deraf følger. Ikke mindst det forstærkede fokus på den registreredes rettigheder. Vi frygter det vil føre til en lavine af mennesker, der ønsker at få udleveret optagelser af dem selv.

Udleveringen vil i sig selv blive belastende, men det virkelige problem er, at der meget ofte optræder andre mennesker på billederne. Deres data må jo ikke udleveres, så i praksis betyder det, at alle andre end den registrerede, der har bedt om billederne, skal "afmaskes". Afhængigt af tv-overvågningsanlæggets alder og beskaffenhed vil dette enten være umuligt eller forbundet med store omkostninger. Der findes i dag ingen anlæg på markedet, hvor afmaskning ikke kræver store ressourcer.

Som det beskrives på side 151 i bemærkningerne til lovforslaget åbner forordningen op for, at medlemsstaterne i national lovgivning kan begrænse retten til indsigt for den registrerede. Af bemærkningerne fremgår det at "I afvejningen om særligt undtagelse fra indsigtsretten efter forordningens artikel 15 indgår som nævnt på den ene side den registreredes interesse i at få kendskab til oplysningerne. Hermed sigtes ikke blot til den registreredes interesse i kendskab til oplysningerne i forbindelse med overvejelser om indbringelse af en sag, hvori de indsamlede oplysninger indgår, for domstolene, højere administrativ myndighed, vedkommende tilsynsmyndighed eller Folketingets Ombudsmand, men også til den registreredes interesse i at kunne kontrollere oplysningernes rigtighed med henblik på den dataansvarliges anvendelse af oplysningerne".

Heraf fremgår, at indsigt både kan kræves hvor den registrerede har en særlig interesse i forbindelse med indbringelse af en sag i at få kendskab til oplysningerne, men også hvor han blot vil kontrollere oplysningernes rigtighed med henblik på den dataansvarliges anvendelse. Det kunne også være med henblik på sletning af oplysningerne.

SikkerhedsBranchen foreslår, at for så vidt angår udlevering af billeder fra tv-overvågning, skal der gælde, at man kun kan få disse udleveret, hvis man har den særlige interesse i forbindelse med en konkret hændelse eller sag, man ønsker eller overvejer at indbringe for domstolene etc.

Begrundelsen er:

- Det er forbundet med endog meget store omkostninger at udlevere eller give indsigt i optagelserne. Derfor skal man have en særlig interesse i at bede om at få udleveret billederne. Subsidiært kan man gøre klart, at adgangen til at opkræve et gebyr som beskrevet i forordningens artikel 12 nummer 5 specifikt gælder for de tilfælde, hvor optagelser ønskes udleveret uden særlig interesse. Gebyret skal svare til de faktiske omkostninger ved at udlevere optagelserne.
- Det giver ingen mening at kontrollere eller rette i data. Det der er optaget kan ikke ændres.
- Sletning af oplysningerne sker automatisk i henhold til bestemmelsen i kapitel 6a i den gældende persondatalov, som videreføres i lov om tv-overvågning. Hvis det vurderes at retssikkerheden vil forbedres ved at mindske de nuværende 30 dage, der må gå inden optagelserne skal slettes, til f.eks. 14 dage, vil det ikke betyde noget for SikkerhedsBranchen. Langt de fleste kameraer er installeret af kriminalitetsbekæmpelseshensyn, og her har den dataansvarlige ikke brug for at gemme optagelserne længe.
- Spørgsmålet om den dataansvarliges anvendelse af optagelserne er også reguleret, idet videregivelse i praksis kun må ske til Politiet og billederne ellers ikke må anvendes til andet formål end det de er optaget for (kriminalitetsbekæmpelse).
- Endelig giver de relativt lange svarfrister på den registreredes anmodning ikke megen mening i sammenhæng med et lagrings- eller registreringsmiljø, hvor den gennemsnitlige lagringstid er omkring 14 dage. Optagelserne er med andre ord slettet inden de er fundet frem.

Vi ser frem til følgelovgivningen, hvor det er vores håb at man vil samle alle relevante bestemmelser for tv-overvågning i lov om tv-overvågning.

Med venlig hilsen

Kasper Skov-Mikkelsen

Direktør

Justitsministeriet
Databeskyttelseskontoret
Slotsholmsgade 10
1216 København K

SLAGELSE
KOMMUNE
Center for Teknologi og Digitalisering
Casper Brands Plads 6
4220 Korsør

Tlf.: 58 57 36 00

itd@slagelse.dk
www.slagelse.dk

Høring over udkast til forslag til databeskyttelsesloven

Ref.:
Justitsministeriets skrivelse af 7. juli 2017, sagnr. 2016-7910-0021 dok.: 2346800.

27. juli 2017

Sagsnr.: 330-2017-54062

Kontaktperson:
Michael Ferrold
Tlf.: 58 57 90 28

1. Indledning

I henhold til ref. fremsendes Slagelse Kommune hermed bemærkninger til udkast til forslag til databeskyttelsesloven.

2. Strafferetslige sanktioner.

I henhold til forslag til databeskyttelsesloven § 41 stk. 5 udestår stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder.

Slagelse Kommune finder det uklart, hvorvidt denne bemærkning på sigt betyder, at offentlige myndigheder friholdes for sanktioner i forhold til øvrige paragraffer/artikler samt, eller om det er databeskyttelsesforordningens artikler – især i relation til pålæggelse af administrative bøder (artikel 83), der er gældende for dette område.
Slagelse Kommune finder dette bør afklares og indføres i lovforslaget inden mulighederne for kommentering afsluttes, da det vil være væsentligt for det fremtidige kommunale virke.

I henhold til ministeriets bemærkninger

> "På denne baggrund foreslår Justitsministeriet, at overtrædelser af følgende bestemmelser i forordningen – som oplistet i artikel 83, stk. 4 og 5 – skal kunne sanktioneres strafferetligt i lovforslaget:
> 1) den dataansvarliges og databehandlerens forpligtelser i henhold til artikel 8, 11, 25-39 og 42 og 43
> 2) certificeringsorganets forpligtelser i henhold til artikel 42 og 43
> 3) kontrolorganets forpligtelser i henhold til artikel 41, stk. 4.
> 4) .....

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

skal overtrædelse af databeskyttelsesloven kunne straffes i henhold til artikel 83, stk. 4, 5 og 6. Der er ikke i bemærkningerne anført særlige forhold i relation til offentlige myndigheder.

Det anføres i § 41 stk. 1 og 6, at den dataansvarlige og databehandleren kan straffes med bøde eller fængsel indtil 6 måneder for overtrædelse af deres forpligtigelser. Dataansvarlig er en rolle en kommune altid vil bestride og til tider også rollen som databehandler.
Det bør derfor i en tekst til § 41 stk. 5 eller andet sted i § 41 gøres klart, hvorvidt rollen som dataansvarlig og databehandler behandles særskilt i forhold til begrebet "offentlige myndigheder", da disse begreber normalt vil være sammenfaldende.

Justitsministeriet anfører i bemærkningerne, at det i lovforslaget bør fastsættes, hvilke bestemmelser i forordningen og loven, som er strafbelagt ved overtrædelse.
Slagelse Kommune er enig heri og mener, at det bør ske inden mulighederne for yderligere bemærkninger stoppes. Endvidere bør ovenstående tydeliggøres i lovforslaget og/eller med tydeligt reference til databeskyttelsesforordningen.

3. Adfærdskodekser

I henhold til databeskyttelsesforordningen artikel 40 stk. 1. fremgår det, at

> "Medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen tilskynder til udarbejdelse af adfærdskodekser, der under hensyntagen til de særlige forhold i de forskellige behandlingssektorer og mikrovirksomheders og små og mellemstore virksomheders specifikke behov bidrager til korrekt anvendelse af denne forordning."

I henhold til Justitsministeriets betænkning nr. 1565 af 24. maj 2017 er disse regler mere detaljeret og begrænser sig – i modsætning til persondataloven – ikke nødvendigvis til private dataansvarlige. Der er i vidt omfang tale om en nyskabelse i forhold til gældende ret.

Af betænkningen fremgår endvidere, at der i dag findes nogle tilsvarende regler i persondatalovens § 74, men at denne indtil videre ikke har haft nogen praktisk betydning i Danmark. Dette synes også i et vist omfang at være tendensen i de øvrige EU-medlemsstater. I hvert fald har Kommissionen bl.a. udtalt, at muligheden for udarbejdelse af adfærdskodekser, hidtil sjældent er blevet anvendt.

Det fremgår yderligere af betænkningen, at det stadig er frivilligt, om man vil følge en godkendt adfærdskodeks eller ej, men at overholdelse

SLAGELSE
KOMMUNE

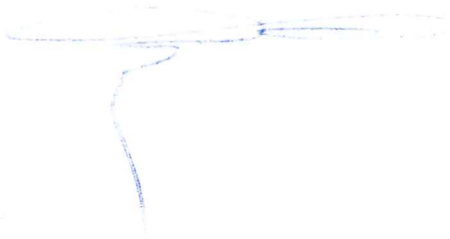
af godkendte kodekser fremadrettet kan bruges til at påvise den dataansvarliges overholdelse af sine forpligtigelser i henhold til forordningen. Det kan samtidig lette arbejdet med implementeringen af forordningen og eventuelt medvirke til reducering af en bødes størrelse.

Slagelse Kommune mener ikke, at det er helt klart, hvad hele dette område egentligt skal omfatte og hvem, der er ansvarlig for udarbejdelse. Jf. artikel 40, stk. 2 tales der om sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, og jf. stk. 5 skal det til udtalelse og godkendelse ved tilsynsmyndigheden.

Det er derfor Slagelse Kommunes opfattelse, at en tydeliggørelse af anvendelsen af adfærdskodekser bør fremgå af den nationale lovgivning.

Venlig hilsen

Claus Ritter
Stabschef CIO



Fra: Steffen Andersen [steffen.a@mail.dk]
Sendt: 21. august 2017 22:29
Til: Justitsministeriet
Emne: Fwd: Bemærkninger til lovforslag om databeskyttelsesloven.
Vedhæftede filer: Høringssvar_dataforordnng_tillaeg_v6.doc

Ifølge hoeringsportalen.dk skal bemærkningerne i vedhæftede brev afleveres på e-mail adressen databeskyttelseskontoret@jm.dk.

Når jeg gør det, får jeg en e-mail tilbage fra postmaster i kriminalforsorgen, at e-mailen ikke kan afleveres, fordi jeg ikke er autoriseret til at anvende den e-mail adresse.

Jeg kan ikke se af e-mailen hvad postmaster på Kriminalforsorgen har at gøre med Databeskyttelseskontoret.

Kan jeg bede om, at Justitsministeriet generelle postkasse videresender mine bemærkninger til lovforslaget til Databeskyttelseskontoret.

På forhånd tak og undskyld ulejligheden.

-------- Forwarded Message --------
Subject: Bemærkninger til lovforslag om databeskyttelsesloven.
Date: Mon, 21 Aug 2017 22:13:32 +0200
From: Steffen Andersen <steffen.a@mail.dk>
To:databeskyttelseskontoret@jm.dk

Vedhæftet i Microsoft word format.

Med venlig hilsen

Steffen Andersen

Justitsministeriet
Databeskyttelseskontoret
Slotsholmsgade 10
1216 København K

databeskyttelse@jm.dk

Høringssvar vedr. udkast til forslag til databeskyttelsesloven

22. august 2017

Søren E. Frandsen
Chef, SDU RIO
sfr@sdu.dk
T +4565501075
M +4529258690

Syddansk Universitet (SDU) har den 7. juli 2017 modtaget Justitsministeriets høringsbrev for udkast til forslag til databeskyttelsesloven. SDU takker for muligheden for at deltage i høringen og sender hermed sine bemærkninger.

SDU finder det afgørende for universiteternes fortsatte virke og bidrag til det danske samfund, at særreglerne for videnskabelige og statistiske undersøgelser, som foreslået i § 10, stk. 1-3, vedtages. Disse paragraffer er centrale for, at SDUs forskere fortsat kan bruge følsomme personoplysninger i forskningen til gavn for borgere, erhvervsliv og samfund i øvrigt. SDU opfodrer til, at den nuværende praksis, hvor offentlige forskningsinstitutioner har bemyndigelse til at tillade videregivelse af personoplysninger omfattet af § 10 inden for Danmark, vil blive videreført efter 25. maj 2018.

For så vidt angår videregivelse af oplysninger omfattet af § 10 til tredjelande, opfordrer SDU til, at den nuværende praksis lempes. Det understreges i den forbindelse, at det er vitalt for forskningen og anvendelsen af den, at universiteterne fortsat vil kunne samarbejde internationalt, inklusiv at videregive under regulerede forhold følsomme personoplysninger til tredjelande, som foreslået i § 10, stk. 3. Som det anføres i betænkning nr. 1565, bind 1, side 103, gives der som altovervejende udgangspunkt ikke tilladelse til at videregive oplysninger til dataansvarlige i tredjelande. Denne praksis forhindrer i høj grad danske forskningsinstitutioner i at samarbejde med bl.a. amerikanske institutioner, herunder muligheden for at hjemtage midler fra f.eks. National Institutes of Health (NIH).
Da selve reguleringen af sikre og usikre tredjelande er et EU-anliggende, opfodrer SDU til, at det bliver muligt for danske forskningsinstitutioner under Databeskyttelsesloven at videregive oplysninger til tredjelande, hvis forskningsinstitutionen sikrer, at modtageren har accepteret EU-Kommissionens standardkontrakter eller har tilsluttet sig EU-U.S. Privacy Shield.

SDU finder det tilsvarende vigtigt af hensyn til den registreredes vitale interesser, som foreslået i udkastets § 10, stk. 4, som giver mulighed for at orientere den regi-

Syddansk Universitet
Campusvej 55
5230 Odense M
T +45 6550 1000
www.sdu.dk

strerede om livstruende og alvorlige sygdomme, også vedtages. Det er universitetets klare opfattelse, at denne bestemmelse blandt andet er afgørende for at omsætte meget af den danske registerforskning til bedre og nye behandlingsmetoder til gavn for patienter og samfundsøkonomi.

Det er vigtigt for, at ovenstående i praksis kan gavne dansk forskning og mulighederne for at arbejde med persondata, at undtagelsen til den registreredes indsigtsret i videnskabelige og statistiske undersøgelser, som foreslået i § 22, stk. 5, også vedtages.

SDU bemærker, at efter som Datatilsynet tidligere har accepteret, at videnskabelige medarbejdere på offentlige forskningsinstitutioner kan være dataansvarlige for behandling af personoplysninger som led i deres ansættelse, så bør det præciseres, at dataansvaret efter databeskyttelsesloven påhviler forskningsinstitutionen og ikke den videnskabelige medarbejder.

Det er SDUs tolkning, at Databeskyttelsesforordningen lægger op til, at anmeldelsesordningen afskaffes, men i artikel 36, stk. 5, får medlemsstaterne mulighed for under national ret at kræve, at dataansvarlige søger og opnår forudgående tilladelse fra tilsynsmyndigheden i forbindelse med en dataansvarligs behandling under udførelsen af en opgave i samfundets interesse.
SDU mener, at det bør afklares, om behandling af personoplysninger til videnskabelige formål, historiske forskningsformål eller statistiske formål skal anmeldes til Datatilsynet efter den 25. maj 2018.

Med venlig hilsen

Søren E. Frandsen
Chef
SDU Research & Innovation Organisation

Fra: Thomas Finne Andersen [ThomasAndersen@Shret.dk]
Sendt: 25. august 2017 11:48
Til: £Databeskyttelseskontoret (951s26)
Emne: Høring over udkast til forslag til følgebrev til databeskyttelsesloven - (2017-7910-0034)

Sø- og Handelsretten har ingen bemærkninger.

Med venlig hilsen

Thomas Finne Andersen
Konstitueret juridisk chef
Direkte: + 45 99 68 47 13
ThomasAndersen@Shret.dk

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

Vestre Landsret
Præsidenten

Justitsministeriet
Lovafdelingen
Slotsholmsgade 10
1216 København K

Sendt pr. mail til databeskyttelseskontoret@jm.dk

J.nr. 40A-VL-56-17
Den 05/09-2017

Justitsministeriet har ved brev af 7. juli 2017 (sagsnr. 2016-7910-0021) anmodet om eventuelle bemærkninger til høring over udkast til forslag til databeskyttelsesloven.

Vestre Landsret er bekendt med Østre Landsrets høringssvar og kan tilslutte sig dette.

Med venlig hilsen

Helle Bertung

VIDEN TIL VELFÆRD

DET NATIONALE FORSKNINGS- OG ANALYSECENTER FOR VELFÆRD

Økonomi- og Indenrigsministeriet
Slotsholmsgade 10
1060 København K
Att.: Maja Bæk Andersen

10. august 2017
Journal nr. 9444
MLA

HØRINGSSVAR VEDRØRENDE FORSLAG TIL NY DATABESKYTTELSESLOV

VIVE – Det Nationale Forsknings- og Analysecenter for Velfærd har modtaget udkast til forslag om ny databeskyttelseslov (supplerende bestemmelser til EU-forordning 2016/679 af 27. april 2016) i høring. I forlængelse heraf har VIVE følgende bemærkninger:

VIVE, hvis kerneområde er forskning og analyse, har med stor tilfredshed noteret sig, at forslaget til ny databeskyttelseslov bevarer råderummet i relation til adgang til og behandling af data, der skal bruges til videnskabelige eller statistiske formål.

Det har stor betydning for VIVEs virksomhed, at der netop er foretaget en afvejning af hensynet til beskyttelse af personlige oplysninger og hensynet til forskning og statistik, således at vi ikke er pålagt unødige administrative og/eller økonomiske byrder, der kunne blive en barriere for gennemførelsen af relevante forsknings- og analyseprojekter.

Ligeledes har VIVE med tilfredshed noteret sig, at regelsættet i relation til HR-data sikrer, at vi kan behandle personoplysninger før, under og efter ansættelsesforholdet i samme omfang som under de nugældende regler.

Med venlig hilsen

Mette Deding
Udviklingsdirektør
mcd@sfi.dk

Østre Landsret
Præsidenten

ØSTRE LANDSRET DANMARKS DOMSTOLE

Den 5 SEP. 2017
J.nr. 40A-ØL-52-17
Init: sdy

Justitsministeriet
Lovafdelingen
Slotsholmsgade 10
1216 København K

Sendt pr. mail til: databeskyttelseskontoret@jm.dk

Justitsministeriet har ved brev af 7. juli 2017 (Sagsnr. 2016-7910-0021) anmodet om eventuelle bemærkninger til høring over udkast til forslag til databeskyttelsesloven.

Efter drøftelse på plenarmøde den 1. september 2017 skal jeg meddele, at landsretten finder, at det på baggrund af forordningens artikel 23, stk. 1, litra f) og j) sammenholdt med præambel 20 og under hensyn til domstolenes særlige status og den detaljerede procesregulering i retsplejeloven bør overvejes at fastsætte generelle undtagelser for oplysningspligten og indsigtsretten for så vidt angår domstolenes judicielle virksomhed, og at bemærkningerne til lovudkastets § 39, stk. 2, 2. led, bør præciseres, herunder således at det tydeligt fremgår, hvilke udfald sager, der indbringes for domstolene efter den pågældende bestemmelse, kan få.

Med venlig hilsen

Bent Carlsen

AALBORG UNIVERSITET

JURAENSHUS

Sten Bønsing
Ph.D.
Lektor i forvaltningsret
Tlf. 99 40 82 69
sb@law.aau.dk

Juridisk Institut
Juraens Hus
Niels Jernes Vej 6 B
9220 Aalborg Øst
www.law.aau.dk

13. august 2017

Justitsministeriet
Databeskyttelseskontoret
Att. Nanna Due Binø
databeskyttelseskontoret@jm.dk

Vedr. høring over forslag til Databeskyttelseslov – j.nr. 2016-7910-0008

På grundlag af ministeriets høring over forslag til databeskyttelseslov fremsendes hermed følgende bemærkninger.

Bemærkningerne vedrører udelukkende lovforslagets § 41, stk. 5, hvorefter bødeansvar for offentlige myndigheder er udeladt af høringsforslaget.

De følgende bemærkninger vedrører derfor synspunkter på, om offentlige myndigheder bør pålægges et bødeansvar for overtrædelse af databeskyttelsesloven.

Det er generelt min opfattelse, at der er en række omstændigheder, der taler imod et bødeansvar på netop dette område.

Indledningsvis skal det nævnes, at præventive grunde generelt (altid) taler for straf. Dette gælder både for offentlige myndigheder og for alle andre.

1. Generelt

Det er *generelt* min opfattelse, at bødeansvar ikke er en egnet straf for offentlige myndigheders overtrædelser af lovgivningen. Dette kan på *enkelte* område være velegnet, men efter min opfattelse er dette ikke udgangspunktet.

Dette skyldes det velkendte forhold, at bødeansvar på offentlige myndigheder i væsentligt omfang bliver et spørgsmål om, at "flytte penge" internt i det offentlige.

2. Myndighedsforpligtelser

Hvis myndigheder pålægges en bøde af en vis betydning, vil den yderste konsekvens være, at myndigheden må beskære dens aktiviteter tilsvarende. Da offentlige myndigheder ikke er sat i verden for at tjene penge, men tværtimod sat til – på Folketingets vegne – at løse ganske bestemte opgaver, vil konsekvensen være, at myndigheden må fravælge en del af de opgaver, som den er blevet pålagt ved lov. For en snæver betragtning vil myndigheden derfor komme i det dilemma, at den skal beskære den opgave, som Folketinget har pålagt den ved lov.

Hvis eksempelvis et hospital (som håndterer mange følsomme personoplysninger) pålægges en betydelig bøde, vil konsekvensen være, at fx operationer må aflyses. Det er således hverken personalet eller hospitalet, der mærker konsekvenserne, men patientbehandlingen, der "straffes".

3. Personligt strafansvar

Der er en meget, meget langt tradition for at pålægge offentligt ansatte er personligt strafansvar for retsstridig håndtering af personoplysninger. I hvert fald tilbage til Danske Lov fra 1683 (bl.a. bestemmelserne 2.-5.-20. og 2.-9.-8. og 2.-9.-26.) har offentligt ansatte kunnet straffes for brud på håndtering af personoplysninger. I straffeloven fra 1866 § 139 fandtes en mere generel regel. Dette er ikke alene teoretisk, men har givet sig udtryk i ganske mange sager. Privatansatte er i realiteten først med persondataloven blevet underlagt et strafansvar for håndtering af personoplysninger (bortset fra visse dele af privatlivsbekyttelsesreglerne i straffeloven).

Efter den nuværende straffelov er offentligt ansattes ansvar bl.a. reguleret i straffelovens § 152 (jf. bl.a. nærmere forvaltningslovens § 27, stk. 1, nr. 1 og stk. 4, nr. 5). Denne anvendes *ofte* til at straffe offentligt ansatte, der håndterer personoplysninger uberettiget.

Herudover er offentligt ansatte i langt videre omfang end private omfattet af et personligt strafansvar, hvis de bryder lovgivningen. Faktisk er udgangspunktet, at *privatansatte* ikke er underlagt et *generelt* strafansvar for pligttilsidesættelser, mens udgangspunktet er, at *offentligt* ansatte er underlagt et sådant generelt ansvar.

Straffelovens §§ 155-157 pålægger således generelt offentligt ansatte strafansvar. Dette gælder principielt for alle typer lovbrud, dvs. både brud på sagsbehandlingsregler, konkrete brud på magtfordrejning m.v. Disse regler dækker også brud på al speciel lovgivning, dvs. miljøregler, sociallovgivning m.v. *Bestemmelserne dækker også misbrug af personoplysninger*.

Fra de senere års praksis kan *eksempelvis* nævntes en dommen fra 9/2 2017, hvor en lokalpolitiker i Københavns Kommune blev dømt for udlevering af personlige oplysninger om en borger.

Tilsvarende kan nævntes en sag fra 2012, hvor en borgmester blev idømt 30 dages *fængsel* (ubetinget) for at skaffe sig personlige oplysninger fra kommunens administration om en politisk modstander under en valgkamp.

Det kan hertil lægges, at der formentlig foreligger endnu flere sager, som er afgjort disciplinært, fx med afskedigelser. Et gæt er her, at der er tale om et antal sager, der er langt højere end antallet af straffesager. Heroverfor må det antages, at privatansatte i realiteten så godt som aldrig sanktioneres disciplinært for brud på persondataregler.

Der er således en ganske lang tradition inden for det offentlig for at pålægge ansatte en personlig straf (strafferetligt eller disciplinært), mens der er tradition for, at der i det private pålægges virksomheder bøder. Dette skyldes det helt grundlæggende forhold, at virksomheder er sat i verden for at tjene penge, mens offentlige myndigheder er sat i verden for at løse bestemte opgaver. Derfor er det mest hensigtsmæssigt, hvis private virksomheder rammes på økonomien, mens offentligt ansatte rammes personligt ved, at de ansatte drages til ansvar for ikke at løse en pålagt opgave eller at misbruge sin stilling.

AALBORG UNIVERSITET

JURAENSHUS

Med venlig hilsen

Sten Bønsing

Fra: Aarhus Retshjælp [post@aarhusretshjaelp.dk]
Sendt: 15. august 2017 13:25
Til: £Databeskyttelseskontoret (951s26)
Emne: Høring over udkast til forslag til databeskyttelsesloven - (2016-7910-0021)

Justitsministeriet, Databeskyttelseskontoret, har i mail af 7. juli 2017 anmodet Aarhus Retshjælp om eventuelle bemærkninger til udkast til forslag til databeskyttelsesloven.

I den forbindelse kan det oplyses, at Aarhus retshjælp ikke har bemærkninger til det fremsendte.

Med venlig hilsen

Christel Stigaard
Daglig leder

Vester Allé 8C
8000 Aarhus C

AARHUS
UNIVERSITET
INSTITUT FOR KLINISK MEDICIN

Justitsministeriet

Høringssvar til:

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

Institut for Klinisk Medicin

Kristjar Skajaa

Institutleder

Dato: 22. august 2017

Direkte tlf.: 78459000
Mobiltlf.: 23613970
E-mail:
kristjar.skajaa@clin.au.dk

Institut for Klinisk Medicin, Health takker for muligheden for at afgive høringssvar i forbindelse med forslaget til databeskyttelsesloven.

Høringsmaterialet har været sendt til Institut for Klinisk Medicin og relevante afdelinger på universitetet, herunder Klinisk Epidemiologisk afdeling og på baggrund heraf har instituttet udarbejdet nedenstående høringssvar.

Instituttet har følgende bemærkninger til forslaget:

Generelt

Det er glædeligt, at forordningen giver et meget vidt råderum for medlemsstaterne til at opretholde og indføre nationale regler om behandling af personoplysning for yderligere at præcisere anvendelsen af forordningens bestemmelser, og at databeskyttelsesloven således som udgangspunkt forbliver som nugældende lovgivning med indførelse af særlovgivning, herunder for registerbaseret forskning.

Aarhus Universitet er således overordnet tilfredse med ordlyden i den nugældende persondatalov, men har oplevet udfordringer med indsamling og videregivelse af persondata i forhold til Aarhus Universitets forskningsmæssige behov. Disse udfordringer opleves fortsat med den nye databeskyttelseslov, ligesom der er opstået ny udfordringer, selv om det fremgår af lovbemærkningerne, at der er sket tiltag til imødekommelse af nogle af disse udfordringer. Herudover kan der ligeledes være forskningsmæssige udfordringer med indsamling og videregivelse af persondata i samspillet mellem databeskyttelsesloven og sundhedsloven.

Aarhus Universitet forstår vigtigheden i, at sundhedsdata beskyttes. Beskyttelsen bør ikke medføre manglende behandling af persondata, men medføre bedre it-sikkerhed og fastholdelse af tillid til forskningen. Der skal findes en måde at behandle data på, hvor den registrerede kan have tillid til brugen af data samtidig med, at hvor forskerne opnår de bedste vilkår for at skabe ny viden.

Ad Afsnit I – Indledende bestemmelser

Kapitel 1 – Lovens materielle anvendelsesområde

I forlængelse af ovenstående er det ligeledes i forbindelse med "oplysningspligt", "indsigtsret" og "retten til at blive slettet" og forholdet mellem databeskyttelsesloven og sundhedsloven vigtigt, at gældende regler kan opretholdes og ikke skal ændres som følge af databeskyttelsesloven, således at forskning ikke umuliggøres.

Ad Afsnit II – Behandlingsregler

Kapitel 3 – Behandling af oplysninger

Dataminimering

Forordningens princip om dataminimering, som fremgår af forordningens artikel 5, stk. 1, litra c og som allerede kendes fra den gældende persondatalovens § 5, fortolkes i dag i praksis af de dataansvarlige myndigheder således, at en forsker skal kunne redegøre for formålet med at behandle hver af de enkelte variable i forhold til beskrivelsen af forskningsprojektets formål, og således meget restriktivt. En sådan restriktiv fortolkning betyder, at alene forskning med hypotesedrevne forskningsmetoder kan gennemføres, og muligheden for at kontrollere yderligere faktorer og gøre nye og uventede fund af potentiel stor betydning for samfundet ikke kan gennemføres.

Med de mange tilgængelige data og stor computerkraft er der kommet nye analysemuligheder, hvor man ikke arbejder ud fra præspecificerede hypoteser, men undersøger de sammenhænge, data selv danner. En forsker kan f.eks. ønske at undersøge eventuelle årsager eller markører til sygdomsmønstre, uden at have en distinkt forventning om hvilke variable, der påvirker sygdomsmønstret. For at udnytte mulighederne i at målrette forebyggelse og behandling, er det nødvendigt, at forskerne har adgang til at analysere store datamængder for at finde nye sammenhænge i sygdomsforløb, som ofte skabes i komplekse samspil med mange faktorer. F.eks. ved at undersøge sammenhænge mellem variabler fra mange registre, biobanker etc. Big Data adskiller sig fra de klassiske registre ved, at datamængderne er så store, at de ikke kan analyseres under den nugældende praksis for registerforskning.

Der henstilles til, at det vurderes, hvorvidt der kan åbnes op for en mindre restriktiv fortolkning og dermed åbnes op for en forskning uden pre-definerede formål, f.eks. i brug af Big Data til forskning i ko-morbiditet, ellers får vi ikke de "tilfældige opdagelser" (serendipitet), som kan give os svar på sammenhæng og mulig forebyggelse til glæde for alle danske borgere.

Videregivelse af data til sundhedsvidenskabelig forskning og statistik

Det er glædeligt, at det foreslås i databeskyttelsesloven § 10, stk. 4 at bemyndige sundhedsministeren til efter forhandling med justitsministeren – og uanset udgangspunktet i stk. 2 – at fastsætte regler om, at oplysninger omfattet af databeskyttelsesforordningens artikel 6 og 9, som er behandlet med henblik på at udføre sundhedsvidenskabelig forskning og statistik senere kan behandles til andre formål end videnskabelige eller statistiske formål, hvis en sådan behandling er nødvendig til varetagelse af den registreredes vitale interesser.

Det fremgår af de specielle bemærkninger i udkastet til lovforslaget, at der er tale om situationer, hvor den registrerede lider af livstruende eller klart alvorlig sygdom, som enten kan behandles, forebygges eller lindres, og det derfor er nødvendigt af hensyn til den registreredes vitale interesser at behandle, herunder videregive oplysningerne med henblik på dels at informere den registrerede om dette fund, dels at benytte oplysningerne til at vurdere, om og i givet fald hvilken patientbehandling som bør iværksættes. Endvidere vil der blive stillet krav om, at der enten skal foreligge et samtykke fra den registrerede (afgivet inden forskningsprojektets påbegyndelse) eller på anden vis være passende foranstaltninger, der sikrer den registreredes interesser og understøtter individbeskyttelse og selvbestemmelse, herunder retten til ikke at vide (f.eks. høring af sagkyndig komité).

Det fremgår ligeledes af de specielle bemærkninger i udkastet til lovforslaget, at bemyndigelsen ligeledes vil kunne blive benyttet til at fastsætte regler, der tillader behandling af sådanne oplysninger i situationer, hvor behandlingen vil være nødvendig af hensyn til varetagelse af den registreredes vitale interesser i forbindelse med valg af konkret patientbehandling, dvs. hvor behandling af oplysningerne sker som beslutningsstøtte for en sundhedspersons beslutning om konkret – skræddersyet – patientbehandling (personlig medicin) til patienter, som lider af livstruende sygdomme, som kan behandles, forebygges eller lindres. Endvidere vil der blive stillet krav om, at der altid skal foreligge et samtykke fra den registrerede.

Endeligt fremgår det af de specielle bemærkninger i udkastet til lovforslaget, at det kan komme på tale på et senere tidspunkt at fastsætte bestemmelser om, at oplysninger, der stammer fra sundhedsvidenskabelige statistiske undersøgelser, ligeledes vil kunne behandles med henblik på varetagelse af den registreredes vitale interesser, f.eks. statistik, der bruges til patientsikkerhedsformål, monitorering mv.

I de registerbaserede studier forsøger man at forudsige prognosen for den enkelte patient ved at studere grupper af lignende patienter. Tidligere blev f.eks. brystkræftpatienter betragtet som en ensartet gruppe med samme sygdom, og alle patienter fik stort set samme behandlingstilbud. I dag skræddersyes behandlingen (personlig me-

dicin) baseret på en lang række specifikke faktorer, hvilket medfører, at når der fortsat skal studeres, hvordan brystkræftpatienter klarer sig, skal patienterne sammenlignes med andre patienter med samme sammensætning af de specifikke faktorer. For at finde gruppen af lignende patienter, skal der være adgang til disse faktorer på alle brystkræftpatienter – ellers risikerer vi at få en skævvredet sammenlignings gruppe. Upræcise eller fejlagtige sammenligningsgrupper giver risiko for, at der tages forkerte beslutninger om, hvad der er bedst for patienternes sundhed.

Det er som ovenfor anført afgørende for nye behandlinger samt personlig medicin, at der er mulighed for adgang til alle data, således at der ikke sker skævvridning i data. Et krav om samtykke kan medføre skævvridning i data og dermed usikre forskningsresultater, idet et samtykke enten kan være en umuligt at opnå, hvis de registrerede enten er døde eller ikke kan findes eller der kan være tale om særligt udsatte grupper, hvor samtykke ikke kan opnås i samme grad. Endeligt kan det resultere i, at analysen vil være umulig at gennemføre.

Der henstilles til, at det vurderes, hvorvidt betingelserne for hvilke typer af sygdomme, de sundhedsvidenskabelige forskningsresultater kan anvendes til patientbehandling, ikke fortolkes for restriktivt, således at f.eks. alene kræftsygdomme tilgodeses.

Der henstilles endvidere til, at det vurderes, hvorvidt et særligt krav om samtykke fra den registrerede i forbindelse med patientbehandling og/eller beslutningsstøtte skal bibeholdes, og i stedet anse patientens samtykke til behandling i sundhedsvæsenet for også at gælde den behandling, der er sket eller skal ske i fremtiden.

Endeligt henstilles der til, at der allerede på nuværende tidspunkt fastsættes regler for behandling af data til brug for til patientsikkerhedsformål, monitorering mv.

Forholdet til sundhedsloven

Der vil i forbindelse med de ovenfornævnte analyser være behov for adgang til data i såvel registre som i patientjournaler, der reguleres af sundhedsloven, idet der vil være behov for at validere registrene. Det er ligeledes her afgørende, at der er mulighed for adgang til alle data.

Adgang kan enten ske ved patientens samtykke til indhentning eller ved et stedfortrædende myndigheds samtykke til videregivelse. Et krav om patientens samtykke kan som ovenfor anført ligeledes få betydning for forskningsresultatet henholdsvis umuliggøre gennemførelse af analysen, idet ikke alle patienter ses regelmæssigt i et ambulatorium eller bliver indlagt på et sygehus, kan være døde eller umulige at finde eller der kan være tale om grupper der er særligt udsatte eller truede, hvor samtykke ikke altid kan opnås.

Et stedfortrædende myndigheds samtykke til videregivelse kan ligeledes være problematisk at finde ud af, hvor man skal have videregivet oplysningerne fra – altså at finde data.

Endvidere må man ikke, hvor data er blevet videregivet med stedfortrædende myndigheds samtykke, efterfølgende henvende sig til patienten for at initiere yderligere undersøgelse, hvis forskningen viser, at en særlig gruppe har klaret sig rigtig dårligt.

Endeligt skal der specielt vedrørende stedfortrædende myndigheds samtykke henvises til bemærkninger under kapitel 1 og 6 omkring "oplysningspligt", "indsigtsret" og "retten til at blive slettet".

Anonymisering/pseudo-anonymisering

Hvor det er muligt at behandle data, der er anonymiseret, vil der ikke være et krav om samtykke.

Det fremgår af præamblens betragtning nr. 26 til persondataforordningen, at anonymisering kræver "uigenkaldelig af-identificering", således at en person hverken direkte eller indirekte kan identificeres. Da der næsten altid vil være mulighed for indirekte identifikation, hvis et datasæt overhovedet skal kunne have et indhold – særligt – men ikke alene - når der er tale om biologiske eller genetiske data (biologisk materiale), vil der være behov for, at persondata kan videregives i en for modtageren ikke umiddelbar personhenførbar form og alligevel være tilstrækkeligt anonymiserede. Dette er bl.a. et problem, når der arbejdes med personlig medicin og rare diseases.

Der henstilles til, at det vurderes, hvorvidt tilstrækkelig anonymisering generelt kan være fjernelse af CPR, navn, adresse m.v., så personen ikke umiddelbart er identificerbar, og at dette også gælder for biologiske og genetiske data, selv om der ved brug af hjælpemidler eller detaljeret personkendskab kan ske identifikation af den pågældende.

Ad afsnit III – Registreredes rettigheder

Kapitel 6 – Begrænsninger i registreredes rettigheder

Begrænsninger i registreredes rettigheder i forhold til sundhedsloven

Jævnfør bemærkningerne til kapitel 1 og 3 omkring "oplysningspligt", "indsigtsret" og "retten til at blive slettet" og vigtigheden af at gældende regler kan opretholdes og ikke skal ændres som følge af databeskyttelsesloven, således at forskning ikke umuliggøres. Der tænkes specielt på sundhedslovens regler om stedfortrædende myndigheds

samtykke og fortolkning af "generelle samfundsinteresser", jfr. databeskyttelsesloven § 22, stk. 2, nr. 5.

Ad afsnit IV – supplerende bestemmelser til databeskyttelsesforordningens kapitel IV

Databeskyttelsesrådgiverens kompetencer

Der henstilles til, at rammerne for databeskyttelsesrådgiverens opgaver yderligere præciseres, jfr. forordningens art. 39.

Ad afsnit VI – Uafhængige tilsynsmyndigheder

Kapitel 10 – Datatilsynet

Overførsel til tredjelande

Der henstilles til, at det præciseres, hvilke særlige tilfælde Datatilsynet kan forbyde, begrænse eller suspendere overførsel af særlige kategorier af oplysninger omfattet af databeskyttelsesforordningens art. 9, stk. 1 til et tredjeland eller en international organisation, jfr. § databeskyttelsesloven § 31.

EU - US Privacy Shield

Der henstilles til, at det præciseres hvorvidt kravet om standardkontraktbestemmelser, jfr. forordningens art. 28, er udtømmende eller om f.eks. US Privacy Shield certificering anerkendes.

Fortegnelse

Endvidere henstilles der til, at det præciseres, hvorledes den fortegnelse, der skal erstatte den nugældende anmeldelsespligt, jfr. forordningens art. 30 skal håndteres i praksis.

Ad afsnit VII – Retsmidler, ansvar og sanktioner

Kapitel 12 – Retsmidler, ansvar og sanktioner

AARHUS
UNIVERSITET
INSTITUT FOR KLINISK MEDICIN

Ansvarsfordeling mellem dataansvarlig og databehandler

Der henstilles til. at det præciseres, hvorvidt det i henhold til art. 82, stk. 5 er muligt at aftale anden indbyrdes ansvarsfordeling, jfr. databeskyttelsesloven § 40.

Venlig hilsen

Kristjar Skajaa
Institutleder

Kopi til:

Dekan Lars Bo Nielsen

AARHUS UNIVERSITET

Til Justitsministeriet

Høring over udkast til forslag til databeskyttelsesloven

Justitsministeriet har ved brev af 7. juli 2017 sendt udkast til forslag til databeskyttelsesloven i høring.

Aarhus Universitet har videresendt høringen til fakulteterne og har på den baggrund modtaget vedlagte bemærkninger af 22. august 2017 fra Klinisk Institut.

Universitetet har ikke modtaget andre bemærkninger til udkastet og henholder sig derfor til vedlagte brev.

Med venlig hilsen

Tove Bæk Jensen
Chefkonsulent

Sekretariat og Jura

Tove Bæk Jensen
Chefkonsulent

Dato: 22. august 2017

Direkte tlf.: +45 8715 2139
Mobiltlf.: +45 2899 2554
E-mail: tbj@au.dk
Web: au.dk/tbj@au.dk

Journal nr.:
2017-061-000024
Afs. CVR-nr.: 31119103
Reference: tbj

Sekretariat og Jura
Aarhus Universitet
Nordre Ringgade 1
8000 Aarhus C

Tlf.: +45 8715 0000
Fax: +45 8715 0201
E-mail: unistab@au.dk
Web: www.au.dk