JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 10. oktober 2019
Kontor: Databeskyttelseskontoret
Sagsbeh: Mikkel Reenberg
Sagsnr.: 2019-0030-2580
Dok.: 1224922

Hermed sendes besvarelse af spørgsmål nr. 310 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 13. september 2019. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Anders Lotterup

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 310 (Alm. del) fra Folketingets Retsudvalg:

> "Vil ministeren angive, hvor langt regeringen er med implementeringen af de forskellige tiltag, der fremgår af beretning om datasikkerhed, afgivet af Retsudvalget den 15. januar 2015, herunder oplyse hvilke tiltag, der er gennemført og hvilke, der er i proces med angivelse af, hvornår tiltagene forventes afsluttet?"

Svar:

1. Retsudvalgets beretning om datasikkerhed sætter et vigtigt fokus. Vi skal konstant være opmærksomme på tilstrækkelig beskyttelse af danskernes personoplysninger, særligt i en tid med hastig teknologisk udvikling.

Jeg kan konstatere, at jeg er enig i en meget stor del af de tiltag og grundlæggende principper, som Retsudvalget beskriver. Samtidig er jeg glad for at kunne konstatere, at en stor del af de foreslåede tiltag og principper allerede er gennemført som led i den lovgivning på databeskyttelsesområdet, som har fundet anvendelse fra 25. maj 2018.

De nye regler i databeskyttelsesforordningen og databeskyttelsesloven afløste således fra 25. maj 2018 persondataloven, som var gældende i januar 2015, hvor Retsudvalget afgav sin beretning.

Efter afgivelsen af beretningen besvarede Justitsministeriet den 14. januar 2016 samlet på vegne af den daværende regering spørgsmål nr. 147 (Alm. del), folketingsåret 2014-15 (2. samling), fra Folketingets Retsudvalg. I besvarelsen af spørgsmål nr. 147 gennemgås Justitsministeriets og andre relevante myndigheders bemærkninger til beretningen. Da besvarelsen af spørgsmål nr. 147 i vidt omfang henviste til de på daværende tidspunkt kommende regler i databeskyttelsesforordningen, vil der også i et vist omfang blive henvist til besvarelsen af spørgsmål nr. 147 i det følgende.

I det følgende vil jeg således redegøre for mine bemærkninger til de seks hovedafsnit i beretningens afsnit 3.1-3.6. Justitsministeriet har desuden indhentet relevante myndigheders bidrag til brug for besvarelsen.

2. Til indholdet af Retsudvalgets beretning bemærkes indledningsvis, at databeskyttelsesforordningens formål dels er at sikre beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, dels at sikre den frie udveksling af personoplysninger i EU.

Der findes en række grundlæggende principper i databeskyttelsesforordningens artikel 5, som altid skal være opfyldte, når man behandler personoplysninger. Principperne indebærer bl.a., at man ikke må behandle personoplysninger i videre omfang, end det er nødvendigt i forhold til de formål, som de behandles (princippet om proportionalitet), og at personoplysningerne skal indsamles til udtrykkeligt angivne og legitime formål. Princippet indebærer også, at personoplysninger altid skal behandles på en rimelig og gennemsigtig måde, og at personoplysninger generelt ikke må opbevares i et længere tidsrum, end det er nødvendigt i forhold til de formål, de behandles.

En overtrædelse af artikel 5, som udgør et grundlæggende og vigtigt princip i databeskyttelsesretten, kan straffes med en bøde på op til 20 mio. EUR efter databeskyttelsesforordningens og databeskyttelseslovens regler.

I tilknytning til disse grundlæggende principper i artikel 5 kan man sige, at der i databeskyttelsesforordningen findes tre yderligere grundlæggende principper.

For det *første* findes der et princip om ansvarlighed (”accountability”). Det indebærer, at det er den dataansvarliges ansvar at sikre og *påvise* overholdelse af databeskyttelsesreglerne, herunder den føromtalte artikel 5.

For det *andet* findes der et princip om gennemsigtighed. Det skal være gennemsigtighed omkring behandlingen af personoplysninger for den registrerede. Dette kommer bl.a. til udtryk i reglerne om oplysningspligt i forordningens artikel 13 og 14, hvorefter den dataansvarlige af egen drift skal oplyse om nærmere bestemte forhold over for den, som der behandles personoplysninger om. Princippet kommer derudover bl.a. til udtryk i artikel 15 om retten til indsigt, hvorefter den registrerede bl.a. har ret til at få oplyst, om der behandles personoplysninger om den pågældende og at få kopi af oplysningerne.

Princippet om gennemsigtighed gælder ikke uden undtagelser, da der efter en konkret vurdering kan foreligge et vægtigere modstående hensyn, eksempelvis til statens sikkerhed eller til strafferetlig efterforskning, således at der kan undtages fra eksempelvis retten til indsigt. Dette følger af databeskyttelseslovens §§ 22-23.

For det *tredje* findes der et princip om en risikobaseret tilgang. Når der behandles personoplysninger, skal det ud fra en risikobaseret tilgang sikres, at

behandlingen sker på et passende sikkerhedsniveau. Dette kommer bl.a. til udtryk i databeskyttelsesforordningens artikel 32, hvorefter man bl.a. ud fra de risici, der er i en bestemt behandlingssituation, skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici. Det følger i den forbindelse af Datatilsynets vejledning om behandlingssikkerhed, at f.eks. egne ansattes interne adgang til personoplysninger skal være begrænset til, hvad den pågældende ansatte har behov for. Et passende sikkerhedsniveau fordrer således, at det bl.a. sikres, at egne ansatte kun får adgang til de personoplysninger, som der konkret er behov for i vedkommendes funktion i den pågældende organisation.

Herudover bemærkes det, at overholdelse af databeskyttelsesreglerne påses af Datatilsynet. Enhver registreret har ret til at klage til Datatilsynet, som udøver sine funktioner i fuld uafhængighed. Denne funktionelle uafhængighed sikrer bl.a., at den registrerede kan udøve sin ret til at klage inden for en betryggende retssikkerhedsmæssig ramme.

3. Om beretningens hovedafsnit 3.1 om overordnede principper for datasikkerhed bemærkes i øvrigt følgende:

Justitsministeriet har indhentet en udtalelse fra Datatilsynet, der i relation til spørgsmålet om vejledning om lovgivning og regulering på databeskyttelsesområdet har oplyst følgende:

> ”1. Datatilsynet er den centrale uafhængige statslige myndighed, der fører tilsyn med databeskyttelsesforordningen og databeskyttelsesloven samt lov om retshåndhævende myndigheders behandling af personoplysninger (retshåndhævelsesloven).
>
> Datatilsynets rolle, kompetencer og opgaver er nærmere fastsat i databeskyttelsesforordningens artikel 51-59. Om Datatilsynets opgaver fremgår det af forordningens artikel 57, at tilsynet – for så vidt angår rådgivning og vejledning – navnlig har til opgave:
>
> - at fremme offentlighedens kendskab til og forståelse af risici, regler, garantier og rettigheder i forbindelse med behandling (litra b),
> - at rådgive det nationale parlament, regeringen og andre institutioner og organer om lovgivningsmæssige og administrative foranstaltninger til beskyttelse af fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling (litra c),
> - at fremme dataansvarliges og databehandleres kendskab til deres forpligtelser i henhold til denne forordning (litra d),
> - at informere om registrerede om udøvelsen af deres rettigheder i henhold til forordningen (litra e), og

- at rådgive om konsekvensanalyser (litra l).

Det er efter Datatilsynets opfattelse afgørende for at sikre en høj beskyttelse af danskernes personoplysninger – og derfor også tilsynets vision – at myndigheder og private kender og overholder reglerne for behandling af personoplysninger, og at borgerne kender og kan bruge deres rettigheder. Datatilsynet gør dette muligt og lettere gennem synlighed, information, dialog og kontrol. Det er samtidig Datatilsynets mission at rådgive om registrering, videregivelse og anden behandling af personoplysninger og føre tilsyn med, at myndigheder, virksomheder og andre dataansvarlige overholder reglerne på området.

Datatilsynets forpligtelse til at yde en serviceorienteret og anvendelig rådgivning er ikke kun en del af Datatilsynets vision og mission. Det følger således som nævnt ovenfor også direkte af databeskyttelsesforordningen, at tilsynet skal fremme offentlighedens kendskab til og forståelse af risici, regler, garantier og rettigheder i forbindelse med behandling, og der skal – som noget nyt – sættes særligt fokus på aktiviteter, der er direkte rettet mod børn. Datatilsynet skal endvidere fremme dataansvarliges og databehandleres kendskab til deres forpligtelser i henhold til forordningen.

2. I 2016 og 2017 deltog Datatilsynet meget aktivt i bl.a. det hurtigtarbejdende projektarbejde, som efter vedtagelsen i EU af bl.a. databeskyttelsesforordningen i april 2016 blev iværksat i regi af Justitsministeriet med henblik på at tilpasse dansk lovgivning til forordningen. Datatilsynet bidrog således væsentligt til betænkning nr. 1565 om databeskyttelsesforordningen, der blev offentliggjort den 24. maj 2017 som et resultat af projektarbejdet.

Af betænkningens indledning fremgår på side 14 bl.a., at betænkningen – ud over at tjene det formål at sikre forordningens korrekte gennemførelse i dansk ret og danne grundlag for udarbejdelsen af en ny version af persondataloven og følgelove med konsekvensrettelser – også er tiltænkt at være det retlige grundlag for udarbejdelse af praktisk anvendelige vejledninger.

Datatilsynet var i forlængelse af betænkningen i 2017 ansvarlig for offentliggørelse af 5 nationale vejledninger om forordningen, ligesom tilsynet samme år i regi af den tidligere såkaldte Artikel 29-gruppe (nu Det Europæiske Databeskyttelsesråd) bidrog til udarbejdelse af 5 fælleseuropæiske vejledninger om reglerne.

I 2016 lancerede Datatilsynet også en ekstra hjemmeside, der var dedikeret til bl.a. databeskyttelsesforordningen, og hvor der løbende blev offentliggjort nyheder om arbejdet med forordningen i Danmark og i EU. Herudover offentliggjorde tilsynet et

dokument indeholdende 12 spørgsmål, man som dataansvarlig med fordel allerede på dette tidspunkt kunne begynde at forholde sig til for at forberede sig, inden databeskyttelsesforordningen begyndte at finde anvendelse.

3. Datatilsynet har også i 2018 og 2019 brugt betydelige ressourcer på at rådgive og vejlede om de nye databeskyttelsesregler. Det gælder herhjemme, hvor tilsynet hver dag håndterer mange telefoniske og skriftlige forespørgsler, og samtidig hermed løbende træffer afgørelser i konkrete klagesager, der kan tjene som vejledning for andre, og udarbejder vejledninger mv. Det har i den forbindelse været vigtigt for Datatilsynet at imødekomme det øgede behov for telefonisk rådgivning, som tilsynet i særlig grad oplevede efter den 25. maj 2018, hvorfor Datatilsynet fra og med den 4. september 2018 har udvidet telefontiden med 5 yderligere timer pr. uge, ligesom der er flere medarbejdere til at tage telefonerne.

I 2018 offentliggjorde Datatilsynet endvidere 8 nationale vejledninger om forordningen, som et foreløbigt supplement til de 5 vejledninger, som tilsynet som nævnt ovenfor offentliggjorde om forordningen i 2017. Herudover har tilsynet i 2018 og 2019 – i regi af Det Europæiske Databeskyttelsesråd – bidraget til udarbejdelsen af en lang række fælleseuropæiske vejledninger mv. om reglerne. Alle de nævnte vejledninger kan sammen med en række praktisk anvendelige skabeloner til opfyldelse af oplysningspligten, en databehandleraftale og en aftale om delt dataansvar findes på Datatilsynets hjemmeside.

Datatilsynet lancerede også en ny hjemmeside i maj 2018. Den nye hjemmeside har fået et helt nyt visuelt udtryk og en ny struktur, ligesom alle tekster er nye. Fokus har bl.a. været på at formidle databeskyttelsesreglerne og Datatilsynets praksis mv. på en mere forståelig og brugervenlig måde sammenholdt med den tidligere hjemmeside. Datatilsynet bruger også aktivt tilsynets LinkedIn-profil (9.800 følgere pr. 25. september 2019) til at komme ud med rådgivning og vejledning.

Herudover holder Datatilsynet mange møder med bl.a. interesse- og brancheorganisationer, men også enkeltstående dataansvarlige og databehandlere, hvis der måtte være behov herfor.

Datatilsynet prioriterer endvidere at komme ud og deltage med indlæg mv. på konferencer, seminarer o. lign for at informere om de nye databeskyttelsesretlige regler og tilsynets praksis, men også for, at tilsynet kan opnå større viden om, hvilke udfordringer de registrerede, andre offentlige myndigheder og den private sektor oplever inden for databeskyttelsesområdet. Datatilsynet deltog i 2018 således med indlæg mv. på 67 konferencer, seminarer o. lign.; en fordobling sammenlignet med 2017, hvor tallet var 34. Datatilsynet har også i 2019 allerede nu del-

taget med mange indlæg mv. på konferencer, seminarer o. lign, ligesom tilsynet i juni måned deltog i Folkemødet på Bornholm, efterfulgt af Ungdommens Folkemøde i begyndelsen af september i Valby, og den 3.- 4. oktober 2019 vil Datatilsynet deltage med en stand på Digitaliseringsmessen i Odense, hvor målgruppen den første dag er de offentlige myndigheder, og dagen efter private virksomheder.

Herudover lancerede Datatilsynet og Erhvervsstyrelsen sammen i begyndelsen af 2018 på Virk Startvækst en ny udgave af PrivacyKompasset, så virksomhederne kan få hjælp til at efterleve de nye databeskyttelsesregler. På PrivacyKompasset kan virksomheder således bl.a. tage en online test, der kan hjælpe dem i gang med at implementere databeskyttelsesreglerne i deres organisation og få svar på helt basale spørgsmål i forhold til ansvarlig datahåndtering. PrivacyKompasset er derfor en hjælp til bedre brug af data inden for lovgivningens rammer og åbner samtidigt for, at virksomhederne på længere sigt kan bruge "privacy" som et konkurrenceparameter. Datatilsynet og Erhvervsstyrelsen forventer i øvrigt inden udgangen af 2019 at lancerer en opdateret og videreudviklet version af PrivacyKompasset.

I slutningen af oktober 2018 lancerede Erhvervsstyrelsen og Digitaliseringsstyrelsen endvidere en ny informationsportal, hvor borgere, virksomheder og myndigheder kan finde viden, vejledning og konkrete værktøjer til en sikker digital hverdag. Datatilsynet er en af bidragsyderne til portalen under de punkter, hvor bl.a. myndigheder kan få information om databeskyttelse.

Særligt for brugere af CAMPUS – den offentlige e-læringsplatform – har Datatilsynet endvidere i 2018 sammen med Moderniseringsstyrelsen udviklet et e-læringskursus i databeskyttelsesforordningen. De første moduler blev lanceret i maj 2018. Datatilsynet forventer endvidere inden for de næste 3-4 måneder at offentliggøre en række webinarer om databeskyttelsesreglerne på tilsynets hjemmeside, som alle vil kunne tilgå med henblik på at tilegne sig en grundlæggende viden om reglerne.

Datatilsynet har i 2018 også i samarbejde med nonprofitorganisationen e-mærket udarbejdet en podcast (6 episoder) om reglerne om databeskyttelse, der særligt henvender sig mod små og mellemstore virksomheder. De to første episoder blev lanceret i april og den sidste i oktober 2018. Datatilsynet planlægger inden for kort tid i øvrigt at lancere endnu en podcast, der skal hjælpe mindre virksomheder til at få et overblik over reglerne i databeskyttelsesforordningen. Podcasten består af 15 episoder, og i hvert afsnit indtager forskellige medarbejdere fra Datatilsynet rollen som vært og fortæller om et emne, der er særligt relevant for små og mellemstore virksomheder.

Endelig forventer Datatilsynet inden for kort tid at offentliggøre

10 små animerede videoer om databeskyttelsesreglerne, der er målrettet danskerne generelt (3 videoer, der skal bidrage til mere generelt at gøre danskerne opmærksomme på reglerne og 7 videoer om de registreredes rettigheder).

4. Datatilsynet arbejder i disse år på at blive bedre til – som en yderligere opfølgning på Datatilsynets tilsynsaktiviteter – at bruge den viden, som tilsynet har fået ved de forskellige stikprøvekontroller, som Datatilsynets tilsynsaktiviteter nødvendigvis må være udtryk for, aktivt og omsætte den til yderligere rådgivning og vejledning til såvel de registrerede som de dataansvarlige.

Hvis det f.eks. kan konstateres, at alle de dataansvarlige, som Datatilsynet på et givet tidspunkt måtte have "trukket ud" til et tilsyn, hvor det kontrolleres, at de efterlever reglerne om de registreredes rettigheder – i dette tilfælde oplysningspligten – har svært ved dette, eller hvis tilsynet oplever, at der ses en tendens til, at et bestemt område af databeskyttelsesretten volder de dataansvarlige særlige problemer, bør Datatilsynet sætte ind med yderligere rådgivning og vejledning på de nævnte områder. Efter Datatilsynets opfattelse vil dette også kunne bidrage yderligere til, at myndigheder og private kender og overholder reglerne for behandling af personoplysninger, og at borgerne kender og kan bruge deres rettigheder."

Det følger desuden af Retsudvalgets beretning, at dansk registerforskning er af stor betydning, men at borgeres ret til privatliv og datasikkerhed bør prioriteres, f.eks. gennem anonymisering og pseudonymisering. Justitsministeriet har til brug for besvarelsen af denne del indhentet en udtalelse fra Sundheds- og Ældreministeriet, der har oplyst følgende:

"Sundheds- og Ældreministeriet kan for så vidt angår princippet om, at dansk registerforskning er af stor betydning, men at borgermes ret til privatliv og datasikkerhed bør prioriteres, f.eks. gennem anonymisering og pseudonymisering, henvise til ministeriets tidligere bidrag til Justitsministeriets svar på spørgsmål nr. 147 (Alm. del) af 14. januar 2016.

Sundheds- og Ældreministeriet skal således fastholde, at udlevering af data, der indeholder personoplysninger om patienters helbredsforhold mv., til brug for forskning på sundhedsområdet, herunder registerforskning, som udgangspunkt ikke bør ske i personhenførbar form, medmindre det godtgøres, at et givent forskningsprojekt ikke kan gennemføres alene på baggrund af ikke personhenførbare oplysninger.

På sundhedsområdet arbejdes der fortsat med øget brug af pseudonymisering af personoplysninger til forskningsprojekter, eksempelvis gennem såkaldte forskermaskineløsninger.

> Sundheds- og Ældreministeriet kan i den forbindelse nævne, at en ny procedure for forskermaskine-løsningen i Sundhedsdatastyrelsen blev vedtaget og idriftsat i januar 2018. Den nye procedure indebærer, at forskere, der ønsker adgang til registre, som Sundhedsdatastyrelsen er ansvarlig for, som udgangspunkt kun kan få adgang til disse via en forskermaskine-løsning. Når Sundhedsdatastyrelsens forskermaskine-løsning anvendes til registerforskning indebærer det, at forskeren kun kan få adgang til data i pseudonymiseret form, dvs. at cpr-nummer og andre direkte identifikatorer er krypterede. Den nye løsning indebærer yderligere, at adgangen til et givent register i Sundhedsdatastyrelsen vil være afgrænset til lige præcis den del af registeret, som er relevant for det givne forskningsprojekt.
>
> Sundheds- og Ældreministeriet støtter således fortsat en yderligere brug af anonymisering og pseudonymisering, samtidig med at ministeriet finder det vigtigt at fastholde, at visse forskningsprojekter ikke lader sig gennemføre uden brug af personhenførbare oplysninger, herunder f.eks. klinisk forskning, hvor øvrig lovgivning i øvrigt i øvrigt bidrager til beskyttelsen af individet."

I forhold til princippet om, at forskning i datasikkerhed og kryptering bør prioriteres, har Justitsministeriet indhentet en udtalelse fra Uddannelses- og Forskningsministeriet, der har oplyst følgende:

> "Forskning inden for cyber- og informationssikkerhed er blevet prioriteret blandt de statslige forskningsmidler. Senest ved aftale i efteråret 2018 mellem alle Folketingets daværende partier om fordeling af forskningsreserven for 2019 blev der afsat 215 mio. kr. i regi af Danmarks Innovationsfond til forskning i nye teknologiske muligheder.
>
> Midlerne skal understøtte udviklingen af det digitale fagområde og som udgangspunkt bidrage til – bl.a. tværdisciplinær – forskning i eksempelvis kunstig intelligens, big data, Internet of Things, kvantecomputing, it-sikkerhed, blockchain og digital omstilling.
>
> Endvidere blev der med samme aftale afsat 80 mio. kr. til digitale teknologier som kunstig intelligens (AI), big data, Internet of Things og it-sikkerhed med fokus på kapacitetsopbygning af den danske talentmasse på det det digitale område."

Om spørgsmålet om, hvorvidt der bør være en indberetningspligt ved tab af kontrol med følsomme og fortrolige personoplysninger, og om der bør være en instans, som følger op på datasikkerhedsbrud samt gør erfaringerne til-

gængelige for øvrige myndigheder og virksomheder, har Justitsministeriet indhentet en udtalelse fra Datatilsynet, der har oplyst følgende:

> "Med databeskyttelsesforordningens artikel 33 er der indført en generel forpligtelse for alle dataansvarlige til at anmelde brud på persondatasikkerheden til Datatilsynet. Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet. Foretages anmeldelsen til Datatilsynet ikke inden for 72 timer, skal den ledsages af en begrundelse for forsinkelsen.
>
> Udgangspunktet er, at brud på persondatasikkerheden altid skal anmeldes, medmindre det er usandsynligt, at det pågældende brud indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
>
> Et brud på persondatasikkerheden er i forordningens artikel 4, nr. 12, defineret som et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
>
> Databeskyttelsesforordningens artikel 33, stk. 3 og 4, indeholder de nærmere regler for indholdet af anmeldelsen efter stk. 1, og den dataansvarlige skal i den forbindelse bl.a. beskrive karakten af bruddet på persondatasikkerheden og de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet, herunder, hvis det er relevant, foranstaltninger for at begrænse bruddets mulige skadevirkninger.
>
> Foruden forpligtelsen til at anmelde brud på persondatasikkerheden til Datatilsynet, er den dataansvarlige forpligtet til at underrette den registrerede om bruddet, når bruddet sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, jf. forordningens artikel 34, stk. 1.
>
> Anmeldelse af brud på persondatasikkerheden til Datatilsynet sker via den fællesoffentlige indberetningsportal virk.dk.
>
> Datatilsynet udgiver herefter kvartalsvist en oversigt over anmeldelser af brud på persondatasikkerheden, dog sådan at første oversigt vedrørte perioden 25. maj 2018 til 31. december 2018 henset til, at databeskyttelsesforordningen har fundet anvendelse fra den 25. maj 2018.
>
> I perioden 25. maj til 31. december 2018 modtog Datatilsynet 2780 anmeldelser om brud på persondatasikkerheden. Datatilsynet har i perioden fra 1. januar til 31. marts 2019 modtaget 1.521 anmeldelser om persondatasikkerhedsbrud, ligesom tilsynet i perioden fra 1. april til 30. juni 2019 har modtaget 1.740 anmeldelser.

> Datatilsynets kvartalsvise opgørelse over anmeldelser af brud på persondatasikkerheden ledsages af en gennemgang af, dels hvordan anmelderne fordeler sig på de forskellige sektorer, både for så vidt angår offentlige og private dataansvarlige, dels hvad der karakteriserer de forskellige anmeldelser. Det sker navnlig med henblik på, at de dataansvarlige kan drage læring fra de anmeldte brud på persondatasikkerheden og evaluere egne organisatoriske og tekniske foranstaltninger og eventuelt implementere yderligere foranstaltninger med henblik på at undgå tilsvarende brud.
>
> De anmeldte brud på persondatasikkerheden udgør endvidere et værdifuldt datagrundlag, som Datatilsynet benytter i forbindelse med sin tilsynsvirksomhed, herunder ved udvælgelsen af hvilke dataansvarlige som skal være genstand for Datatilsynets tilsyn."

Erhvervsministeriet har over for Justitsministeriet oplyst, at man i relation til spørgsmålet om indberetningspligt på teleområdet kan henholde sig til bidraget i afsnit 2.9 i besvarelsen af spørgsmål nr. 147.

I forhold til beretningens spørgsmål om, hvorvidt lovgivningsinitiativer bør være teknologineutrale, og at anvendelsen af personoplysninger samt konsekvenser for privatlivets fred – herunder hvordan negative konsekvenser for privatlivets fred kan undgås – bør fremgå af bemærkningerne til det fremsatte lovforslag, bemærkes det, at det følger af præambelbetragtning nr. 15 til databeskyttelsesforordningen, at reglerne i forordningen *er* teknologineutrale. Databeskyttelsesloven er også teknologineutral.

Det er desuden min opfattelse, at spørgsmål om behandling af personoplysninger, herunder hjemmelsgrundlaget for behandling af personoplysninger samt konsekvenser for privatlivets fred, fortsat og i overensstemmelse med besvarelsen af spørgsmål nr. 147, afsnit 2.11, i relevant omfang bør fremgå af bemærkningerne til et fremsat lovforslag.

4. Om beretningens hovedafsnit 3.2 om tilsynet med overholdelse af persondataloven bemærkes følgende:

I forhold til spørgsmålet om, hvorvidt Datatilsynets kontrolbesøg skal være risikobaserede, har Justitsministeriet til brug for besvarelsen indhentet en udtalelse fra Datatilsynet, der har oplyst følgende:

> "Efter databeskyttelsesforordningens artikel 57, stk. 1, litra a, skal Datatilsynet føre tilsyn med og håndhæve anvendelsen af forordningen.

> I den forbindelse er det et vigtigt element i Datatilsynets kontrol og tilsynsvirksomhed at foretage varslede tilsyn, herunder særligt tilsynsbesøg, og Datatilsynet har siden den 25. maj 2018, hvor databeskyttelsesforordningen fandt anvendelse, tilstræbt at gennemføre et vist antal varslede tilsyn til trods for, at Datatilsynets fokus primært har været rettet imod vejledningsindsatsen.
>
> Siden databeskyttelsesforordningens anvendelse har Datatilsynet fortsat gennemførelsen af sine varslede tilsyn på baggrund af den strategi, som tilsynet vedtog for 2016-2018.
>
> Tilsynene planlægges for cirka et halvt år ad gangen, hvor Datatilsynet i første omgang finder frem til, hvilke temaer og myndigheder og virksomhedsbrancher tilsynene skal dække, og herefter finder frem til de enkelte dataansvarlige, som skal være genstand for Datatilsynets tilsyn.
>
> Når Datatilsynet udvælger, hvilke temaer og myndigheder samt virksomhedsbrancher tilsynene skal dække, fokuserer Datatilsynet navnlig på behandlinger af personoplysninger, som på grund af deres formål, omfang eller karakter indebærer en særlig risiko for at krænke de registreredes ret til databeskyttelse og privatliv, samt på behandlinger, som indebærer brug af ny teknologi. Andre parametre indgår imidlertid også i Datatilsynet vurdering, herunder f.eks. områder, hvor der har vist sig at være udfordringer, henvendelser fra borgere og medier mv. omkring specifikke problemstillinger og en vis geografisk spredning.
>
> Datatilsynet arbejder således allerede med en risikobaseret tilgang til sin tilsynsvirksomhed, men ønsker og arbejder på yderligere at styrke sin tilsynsvirksomhed og sikre en optimal kapacitetsudnyttelse med henblik på at frembyde størst mulig databeskyttelse for de registrerede personer.
>
> På den baggrund har Datatilsynet – i forbindelse med tilsynets igangværende projekt om en ny samlet strategi for Datatilsynet – tillige igangsat en evaluering af Datatilsynets tilsynsvirksomhed."

I forhold til anbefalingen om, at det overvejes, om der bør etableres en klageinstans til at behandle klager over Datatilsynets afgørelser, er det min opfattelse, at Datatilsynet, der som nævnt i afsnit 2 udøver sin tilsynsfunktion i fuld uafhængighed, sikrer retssikkerhed for både de registrerede samt for de borgere og virksomheder, som tilsynet generelt kommer i berøring med ved udøvelsen af sin tilsynsfunktion.

På den baggrund er det også min opfattelse, at der ikke er behov for at oprette en sådan klageinstans. Det bemærkes også i den forbindelse, at Datatilsynets virksomhed er undergivet Folketingets Ombudsmands kompetence, og at Datatilsynets afgørelser i øvrigt kan indbringes for domstolene i overensstemmelse med grundlovens § 63.

På samme baggrund som nævnt ovenfor finder jeg ikke behov for at ændre Datatilsynets organisatoriske forankring, f.eks. at placere tilsynet under Folketinget.

Jeg bemærker endvidere, at Datatilsynet med finansloven for 2018 blev styrket med 12,5 mio. kr. i 2018, 16,4 mio. kr. i 2019 og 16,8 mio. kr. i 2020 og frem, dels som følge af meropgaver vedrørende databeskyttelsesforordningen mv., dels som en generel styrkelse af Datatilsynet. Der henvises i den forbindelse til besvarelse af spørgsmål nr. 60 til L 68 (databeskyttelsesloven) og L 69 (Konsekvensændringer som følge af databeskyttelsesloven samt medieansvarslovens anvendelse på offentligt tilgængelige informationsdatabaser m.v.), folketingsåret 2017-18.

5. Om beretningens hovedafsnit 3.3 om Datatilsynets sanktionsmuligheder ved brud på datasikkerhed kan der henvises til det, som blev anført i besvarelsen af spørgsmål nr. 147, afsnit 4.

Hertil bemærkes, at det nu efter databeskyttelseslovens § 41 er muligt at pålægge både private og offentlige aktører bøder for overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven. Det bemærkes desuden, at både den dataansvarlige og databehandleren kan ifalde ansvar og pålægges sanktioner efter databeskyttelsesforordningen og databeskyttelsesloven.

Bøderammerne for private aktører for overtrædelse af reglerne er på 10 eller 20 mio. EUR afhængig af hvilke regler, som overtrædes. En bøde kan dog også udgøre op til 2 % af en virksomheds samlede globale omsætning i et forudgående regnskabsår, hvis dette beløb er højere. Det forudsættes i forarbejderne til databeskyttelsesloven, at der som følge af dette betydelige maksimale bødebeløb i forordningen lægges op til en væsentlig forøgelse af bødeniveauet for overtrædelse af de databeskyttelsesretlige regler set i forhold til størrelsen af bøder for overtrædelse af den tidligere gældende persondatalov.

6. Om beretningens hovedafsnit 3.4 om samling af ansvaret for datasikkerhed kan der henvises til det anførte i besvarelsen af spørgsmål nr. 147, afsnit 5.

Det bemærkes supplerende, at det følger af databeskyttelseslovens § 1, stk. 3, at regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysningerne, går forud for reglerne i databeskyttelsesloven.

Regler om behandling af personoplysningerne findes fortsat i et meget vidt og forskelligt omfang i dansk lovgivning, herunder i bekendtgørelser. Det er min opfattelse, at den pågældende regulering af behandling af personoplysninger inden for et bestemt ressort – f.eks. på sundhedsområdet – bør høre under den pågældende minister, som har den største ekspertise til rådighed inden for det bestemte område.

7. Om beretningens hovedafsnit 3.5 om tekniske krav til sikring af følsomme og fortrolige personoplysninger har Justitsministeriet indhentet en udtalelse fra Finansministeriet.

Vedrørende betragtningen om privacy by design, har Finansministeriet oplyst følgende:

> ”Som led i den fællesoffentlige digitaliseringsstrategi 2016-2020 er der i juni 2019 i samarbejde mellem Datatilsynet, Justitsministeriet og Digitaliseringsstyrelsen udarbejdet en vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger. I vejledningen gennemgås databeskyttelsesforordningens art. 32 om behandlingssikkerhed, og der gives en introduktion til privacy-by-design og eksempler på tekniske og organisatoriske foranstaltninger, der kan tages i brug i den henseende.”
>
> Hensynet til borgernes privatliv er et væsentligt princip, når it-systemer udvikles og designes, og det er en grundlæggende præmis, at de statslige myndigheder skal arbejde med privatlivsbeskyttelse. Statens it-projektmodel er obligatorisk at anvende for statslige myndigheder, der igangsætter it-udviklingsprojekter. I statens it-projektmodel forpligtes den statslige myndighed til at gennemføre en sikkerhedsmæssig risikovurdering samt en konsekvensvurdering vedrørende databeskyttelse for et kommende it-udviklingsprojekt.

> Som en del af den samlede risikoafdækning for et statsligt it-projekt skal projektet analysere de risici, som relaterer sig til sikkerheden i og omkring it-løsningen. Såfremt it-løsningen skal behandle personoplysninger, skal projektet rådføre sig med organisationens databeskyttelsesrådgiver (DPO) om behovet for at gennemføre en konsekvensanalyse vedrørende databeskyttelse i overensstemmelse med databeskyttelsesforordningen. Hvis konsekvensanalysen viser, at det kan have store konsekvenser for de registrerede, såfremt der sker en sikkerhedshændelse i forbindelse med brugen af den nye it-løsning, skal Datatilsynet høres inden it-løsningen sættes i værk som foreskrevet i databeskyttelsesforordningen. Databeskyttelsesforordningen gælder for både private og offentlige it-udviklingsprojekter og er således ikke begrænset til større statslige it-projekter.
>
> Som en del af statens it-projektmodel er udarbejdet en tjekliste vedr. cybersikkerhed, som medlemmer af Statens It-råd kan anvende, når der gennemføres risikovurderinger af statslige it-projekter."

Vedrørende betragtningen om sikkerhedsstandarden ISO 27001 har Finansministeriet oplyst følgende:

> "Det har siden 2016 været et krav, at de statslige myndigheder skal implementere og arbejde systematisk efter ISO27001, som er en standard for effektiv informationssikkerhedsledelse. Der er løbende gjort status på indsatsen, og det fremgår, at størstedelen af myndighederne endnu ikke er helt i mål.
>
> For at sikre fuld implementering af ISO27001 følger Digitaliseringsstyrelsen i medfør af den nationale strategi for cyber- og informationssikkerhed 2018-2021 op på statslige myndigheders implementering hvert halve år. Myndigheder, der endnu ikke er i mål, skal aflevere en handleplan, som beskriver hvilke indsatser, der vil blive gennemført med henblik på at sikre fuld implementering af standarden. Handleplanerne forelægges regeringen.
>
> For at understøtte indsatsen med myndighedernes implementering af ISO27001 blev der i 2018 afholdt en fællesoffentlig konference om arbejdet med ISO27001. Der afholdes en konference igen i oktober 2019."

Vedrørende betragtningen om anbefalinger vedrørende kontrol af rollebaseret adgang har Finansministeriet oplyst følgende:

> "Som led i den fællesoffentlige digitaliseringsstrategi 2016-2020 etablerede Digitaliseringsstyrelsen i 2016 et klausulbibliotek med en lang række standardklausuler om sikkerhedsmæssige krav. Formålet med standardklausulerne er at inspirere og

støtte myndighederne i forbindelse med indgåelse af it-kontrakter og dermed forenkle arbejdet med at stille hensigtsmæssige sikkerhedskrav i aftaler og it-kontrakter. Klausulbiblioteket er årligt blevet opdateret i strategiperioden og i 2017 blev klausulbibliotek udvidet med et kravkatalog "Sådan stiller du krav til leverandører om informationssikkerhed".

I 2019 videreudvikles klausulbiblioteket og tilhørende kravkatalog i regi af den nationale cyber- og informationsstrategi 2018-2021. Som led heri udarbejdes obligatoriske minimumskrav for samfundskritiske statslige it-systemer i Danmark."

8. Om beretningens "øvrige bemærkninger" i hovedafsnit 3.6 har Justitsministeriet i forhold til, om der bør igangsættes en udredning af, om der bør være grænser for samtykke, indhentet en udtalelse fra Datatilsynet, der har oplyst følgende:

"Gennemsigtighed er et gennemgående princip i databeskyttelsesforordningen. Det fremgår således af forordningens artikel 5, stk. 1, litra a, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (princippet om lovlighed, rimelighed og gennemsigtighed).

Af præambelbetragtning nr. 39 til databeskyttelsesforordningen fremgår i den forbindelse endvidere, at enhver behandling af personoplysninger bør være lovlig og rimelig. Det bør være gennemsigtigt for de pågældende fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet. Princippet om gennemsigtighed tilsiger, at enhver information og kommunikation vedrørende behandling af disse personoplysninger er lettilgængelig og letforståelig, og at der benyttes et klart og enkelt sprog. Dette princip vedrører navnlig oplysningen til de registrerede om den dataansvarliges identitet og formålene med den pågældende behandling samt yderligere oplysninger for at sikre en rimelig og gennemsigtig behandling for de berørte fysiske personer og deres ret til at få bekræftelse og meddelelse om de personoplysninger vedrørende dem, der behandles.

Foruden det generelle princip om gennemsigtighed i forordningens artikel 5, stk. 1, litra a, findes der også nærmere regler om gennemsigtighed i databeskyttelsesforordningens artikel 12, stk. 1, hvoraf fremgår, at den dataansvarlige skal træffe passende foranstaltninger til at give enhver oplysning som omhandlet i artikel 13 og 14 om behandling til den registrerede i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog.

Endelig fremgår det af forordningens artikel 7, stk. 2, at hvis den registreredes samtykke gives i en skriftlig erklæring, der også vedrører andre forhold, skal en anmodning om samtykke forelægges på en måde, som klart kan skelnes fra de andre forhold, i en letforståelig og lettilgængelig form og i et klart og enkelt sprog.

Princippet om gennemsigtighed kombineret med den højere standard for den registreredes samtykke, som databeskyttelsesforordningen efter Datatilsynets opfattelse har medført, sætter herved de registrerede personer i bedre stand til at udøve kontrol over deres personoplysninger, herunder ved at give eller tilbagekalde et samtykke på et informeret grundlag og gøre brug af deres øvrige rettigheder end tidligere.

Datatilsynet har i øvrigt for nylig opdateret vejledningen om samtykke, som er tilgængelig på tilsynets hjemmeside."

Vedrørende anbefalingen om, at der foretages en kortlægning af eksisterende offentlige registre, og at det i den forbindelse overvejes, om der i nogle tilfælde registreres og opbevares mere data end nødvendigt, kan der henvises til det anførte i afsnit 7.3 i besvarelsen af spørgsmål nr. 147.

I relation til, om der bør udarbejdes en national strategi for den samlede offentlige sektor, har Justitsministeriet indhentet en udtalelse fra Finansministeriet, der har oplyst følgende:

"Der er med den fællesoffentlige digitaliseringsstrategi 2016-2020 gennemført en række indsatser med henblik på at styrke informationssikkerheden hos myndighederne på tværs af den offentlige sektor, herunder en fælles indsats for udbredelse af ISO27001, udarbejdelse af et klausulbibliotek med sikkerhedsmæssige krav, jf. bemærkningerne ovenfor om kontrol af rollebaseret adgang, samt en indsats vedrørende informationssikkerhed og god sikkerhedsadfærd for offentligt ansatte. Indsatserne er forankret i en fællesoffentlig arbejdsgruppe med deltagelse af bl.a. Digitaliseringsstyrelsen, Center for Cybersikkerhed, KL, Danske Regioner og diverse styrelser og ministerier. Der henvises i øvrigt til besvarelsen angående 6.3 og 6.4.

Der er derudover lanceret en national strategi for cyber- og informationssikkerhed 2018-2021. Strategien skal øge den tekniske robusthed og sikre bedre beskyttelse af statens kritiske it-systemer, øge viden og kompetencer hos borgere, virksomheder og myndigheder – bl.a. gennem oprettelsen af en in-formationsportal – samt styrke den nationale koordinering og samarbejdet om informationssikkerhed. Med strategien er igangsat 25 initiativer af national karakter. Der er som led heri ligeledes igangsat seks målrettede strategier for at løfte cyber- og informationssik-

kerheden inden for de samfundskritiske sektorer tele, finans, energi, sundhed, transport og søfart.

Som led i strategien skal der gennemføres en national analyse af cyber- og informationssikkerhedssituationen med henblik på at vurdere, om iværksatte tiltag har den ønskede effekt og om organisering og aktiviteter imødegår udviklingen i trusselsbilleder og de deraf vurderede risici mv. Den nationale strategi følges af en styregruppe bestående af syv ministerier, hvor Finansministeriet og Forsvarsministeriet har delt formandskab.

Vedrørende spørgsmålet om, hvorvidt brugen af cpr-nummeret bør gennemgå en grundlæggende revidering, har Justitsministeriet indhentet en udtalelse fra social- og indenrigsministeren, der har oplyst følgende:

"Jeg kan henholde mig til de bemærkninger, som den daværende social- og indenrigsminister afgav i forbindelse med besvarelsen af 14. januar 2016 af spørgsmål 147 fra Folketingets Retsudvalg.

Jeg finder således, at der fortsat ikke er behov for, at brugen af personnummeret skal gennemgå en grundlæggende revidering. Personnummeret er en ti-cifret kode, som tjener til entydigt at identificere en person, f.eks. i et it-system. Uden personnummeret var det ikke muligt hurtigt og enkelt at skelne den ene Jens Hansen fra den anden.

Det har derimod aldrig været meningen med personnummeret, at det skulle tjene som eneste middel til autentifikation – altså til at fastslå eller bekræfte, at en person er den, vedkommende udgiver sig for at være.

Autentifikation skal i stedet ske ved brug af Nem ID, som netop er kendetegnet ved to-faktor kontrol, og som indebærer et helt andet sikkerhedsniveau. NemID benyttes derfor også til autentifikation i alle offentlige digitale løsninger og i vidt omfang også i det private erhvervsliv. Social- og Indenrigsministeriet stiller også krav om anvendelse af NemID i forbindelse med virksomheders og myndigheders selvbetjeningsløsninger, hvorfra der foretages opslag i CPR.

At afskaffe personnummeret som samme, gennemgående systemnøgle i offentlige og private it-systemer vil være meget dyrt og ineffektivt, og der er efter min opfattelse ikke behov for at afskaffe personnummeret som systemnøgle og erstatte det af en anden nøgle."