JUSTITSMINISTERIET
Lovafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 14. januar 2016
Kontor: Databeskyttelseskontoret
Sagsbeh: Kristian Gyde Poulsen
Sagsnr.: 2015-0030-3755
Dok.: 1714999

Hermed sendes besvarelse af spørgsmål nr. 147 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 31. august 2015.

Søren Pind

/

Jakob Lundsager

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 147 (Alm. del) fra Folketingets Retsudvalg:

> ”Ministeren bedes kommentere på beretning om datasikkerhed og redegøre for, hvilke initiativer ministeren på baggrund af beretningen agter at tage jf. beretning nr. 4 af 15. januar 2015. Spørgsmålet har tidligere været stillet i folketingsåret 2014-15(1. samling), jf. REU alm. del - spm. 400.”

Svar:

1.1. Det bemærkes indledningsvis, at nærværende besvarelse er koordineret med Finansministeriet, Forsvarsministeriet, Erhvervs- og Vækstministeriet, Social- og Indenrigsministeriet samt Sundheds- og Ældreministeriet, som spørgsmålet også er stillet til. Justitsministeriet besvarer således spørgsmålet samlet på regeringens vegne.

1.2. Beretning nr. 4 om datasikkerhed indeholder en række anbefalinger om og opfordringer til initiativer på databeskyttelsesområdet. Beretningen indeholder desuden en række overordnede principper, som ifølge arbejdsgruppen bør være grundlæggende for it- og dataarbejde.

Nedenfor under punkt 1.3 og 1.4 følger regeringens indledende bemærkninger til beretningen. Derefter følger under punkt 2 regeringens bemærkninger til visse af de overordnede principper, som ifølge arbejdsgruppen bør være grundlæggende for it- og dataarbejde. Herefter følger under punkt 3-7 regeringens bemærkninger til beretningens enkelte anbefalinger om og opfordringer til initiativer på databeskyttelsesområdet.

1.3. Det skal indledningsvis understreges, at databeskyttelse er et område, som regeringen tager yderst alvorligt og ønsker at prioritere højt.

Beskyttelse af personoplysninger er af stigende betydning som følge af samfundsudviklingen og de teknologiske muligheder. Et enigt Retsudvalg har med sin beretning om datasikkerhed også bekræftet, at det er et område, der er bred enighed om at prioritere.

Det er også baggrunden for, at Justitsministeriet i samarbejde med Datatilsynet er i gang med at se på Datatilsynets nuværende opgaver og ressourcer med henblik på at tilføre flere penge til Datatilsynet.

Regeringen er enig med Folketingets Retsudvalg i, at afsløringerne af overvågning af en række kongelige og kendte personers brug af kreditkort

mv. skal tages alvorligt. Regeringen er også meget enig i, at det er nødvendigt at undersøge behovet for nye initiativer i forhold til beskyttelse af personoplysninger.

Den tidligere justitsminister bad i 2014 sine embedsmænd om sammen med Erhvervs- og Vækstministeriet (og andre relevante ministerier) at kortlægge beskyttelsen af oplysninger om borgernes elektroniske betalinger mv.

Kortlægningen, der i øjeblikket er i gang med at blive udarbejdet, vil skulle danne udgangspunkt for en bred politisk drøftelse. Den politiske drøftelse vil – som den tidligere justitsminister tilkendegav i forbindelse med besvarelsen af forespørgsel nr. F 36 om beskyttelse af danskernes personoplysninger den 3. juni 2014, hvor et enigt Folketing tilsluttede sig en vedtagelsestekst herom – også omfatte en samlet strategi til sikring af danskernes personoplysninger, som regeringen vil udarbejde på baggrund af den politiske drøftelse.

Den politiske drøftelse blev indledt på et møde den 16. september 2014, hvor det også blev drøftet, hvordan den videre arbejdsproces bedst tilrettelægges. Det blev aftalt, at møderækken fortsætter, så snart kortlægningsarbejdet er afsluttet. Arbejdet med kortlægningen forventes afsluttet i inden udgangen af februar 2016.

Den politiske drøftelse bør efter regeringens opfattelse omfatte alle de politiske partier i Folketinget, ligesom drøftelsen bør omfatte flere af de spørgsmål, som adresseres i Retsudvalgets beretning nr. 4 om datasikkerhed.

1.4. Der foregår i øjeblikket forhandlinger i EU om en ny forordning om databeskyttelse, som skal erstatte det nugældende databeskyttelsesdirektiv fra 1995, og som skal danne den fremtidige retlige ramme for databeskyttelse i EU.

Forslaget til en databeskyttelsesforordning indeholder en generel horisontal regulering af behandling af personoplysninger og skal gælde for både den offentlige og den private sektor. Forslaget indeholder generelle principper for databehandling samt regler om, hvornår behandling af personoplysninger kan ske. Forslaget giver den registrerede en række rettigheder, ligesom det indeholder en indgående regulering af den dataansvarliges og databehandlerens ansvar og pligter. Forslaget indeholder endvidere regler

om overførsel af oplysninger til tredjelande samt regler om uafhængige tilsynsmyndigheder. Endelig indeholder forslaget regler om klageadgang, den registreredes mulighed for erstatning samt detaljerede regler om sanktioner for overtrædelse af forordningens bestemmelser.

En forordning gælder direkte – på samme måde som en lov – i medlemsstaterne, og danske myndigheder, virksomheder og borgere har således pligt til at rette sig efter en forordning. Eventuelle nye krav på nationalt niveau til beskyttelse af personoplysninger ville således meget vel kunne vise sig at skulle ændres, hvis databeskyttelsesdirektivet bliver erstattet af en ny databeskyttelsesforordning. Der blev i december 2015 opnået politisk enighed om EU-Kommissionens forslag til en ny databeskyttelsesforordning. Forordningen forventes formelt vedtaget i løbet af foråret 2016.

Det er på den baggrund – som også nævnt i Justitsministeriets besvarelse af 1. maj 2014 af spørgsmål nr. 898 (Alm. del) fra Folketingets Retsudvalg – ministeriets opfattelse, at det ikke vil være hensigtsmæssigt at iværksætte et arbejde med revision af regler på databeskyttelsesområdet på nuværende tidspunkt.

Det bemærkes i den forbindelse, at det anføres i beretning nr. 4 om datasikkerhed, som Retsudvalget afgav den 15. januar 2015, at Danmark bør påbegynde arbejdet med at gennemføre de dele af forordningen, der på nuværende tidspunkt er enighed om.

Justitsministeriet kan i den forbindelse oplyse, at arbejdet med at gennemføre forordningen allerede nu er i sin indledende fase.

2.1. Beretning nr. 4 om datasikkerhed indeholder i afsnit 3.1 som nævnt en række overordnede principper, som ifølge arbejdsgruppen bør være grundlæggende for it- og dataarbejde.

Justitsministeriet kan i den forbindelse helt overordnet bemærke, at ministeriet anerkender størstedelen af disse principper, som allerede i dag også er afspejlet i gældende ret, herunder i persondatalovens regler. Ministeriet skal dog knytte følgende bemærkninger til enkelte af principperne:

2.2. I forhold til princippet om, at virksomheder og offentlige myndigheder bør have adgang til vejledning om lovgivning og regulering på databeskyttelsesområdet, har Justitsministeriet indhentet en udtalelse fra Datatilsynet, der er den statslige myndighed, som fører tilsyn med persondatalovens

overholdelse. Tilsynet har oplyst følgende:

> ”Det er forudsat i de almindelige bemærkninger til persondataloven, at Datatilsynet i første række bør tage sigte på at kunne udøve sin virksomhed gennem generelle retningslinjer og ved en serviceorienteret rådgivning og vejledning frem for en regulering primært koncentreret om afgørelse af enkeltsager i et traditionelt rekurssystem.
>
> I praksis sikres dette bl.a. ved, at Datatilsynet løbende udarbejder vejledninger, retningslinjer og informationstekster. Endvidere offentliggøres relevante afgørelser og udtalelser på tilsynets hjemmeside.
>
> Datatilsynet bidrager også med oplæg på konferencer og møder, ligesom tilsynet dagligt besvarer spørgsmål fra medierne.
>
> I forhold til konkrete myndigheder og virksomheder giver tilsynet rådgivning og vejledning i telefoniske og skriftlige svar samt på møder.
>
> Datatilsynet kan imidlertid konstatere, at der i stadig større omfang efterspørges vejledning og rådgivning også ud over det, som må anses for tilsynets opgave efter den nuværende lovgivning.
>
> Der er således eksempler på, at myndigheder efterspørger bistand til udformning af lovgivning, fordi databeskyttelsesreguleringen opleves som kompliceret. Der kan også være tale om spørgsmål vedrørende myndigheders organisering og praktiske tilrettelæggelse af databehandlinger. I forhold til private virksomheder ses der eksempler på forespørgsler om bistand til detaljeret at afdække spørgsmål vedrørende nye forretningsmodeller og tekniske løsninger, ligesom der rejses spørgsmål om aftalemæssige forhold til leverandører mv.
>
> Herudover er det nødvendigt for tilsynet løbende at prioritere sin ressourceanvendelse, herunder også i forhold til at yde rådgivning og vejledning, og endelig har det betydning, at tilsynet er klagemyndighed for behandlinger af personoplysninger. Tilsynet kan således ikke udtale sig vejledende i forhold til en myndighed eller virksomhed i tilfælde, hvor der i realiteten er tale om en aktuel eller potentiel klage fra en registreret person. Det er af afgørende betydning, at borgere, der eksempelvis mener sig udsat for behandlinger af personoplysninger i strid med loven, eller som ikke får de oplysninger, de mener at have krav på efter reglerne om de registreredes rettigheder, kan få Datatilsynets vurdering af forholdet ved en egentlig klagesagsbehandling.”

2.3. I forhold til princippet om, at borgere bør kunne få oplyst, hvilke data der er registreret om dem, hvorfor data registreres, hvem der har adgang til disse data, hvem der har anvendt adgangen, og hvad data bliver brugt til, bemærkes, at det følger af persondatalovens § 31, stk. 1, at hvis en person fremsætter begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om, 1) hvilke oplysninger der behandles, 2) behandlingens formål, 3) kategorierne af modtagere af oplysningerne og 4) tilgængelig information om, hvorfra disse oplysninger stammer.

Som nævnt i Justitsministeriets besvarelse af 11. oktober 2013 af spørgsmål nr. 1162 (Alm. del) fra Folketingets Retsudvalg forpligter persondatalovens § 31 alene den dataansvarlige myndighed eller virksomhed til at give borgeren oplysning om kategorierne af modtagere og ikke den konkrete modtager.

Det bemærkes i den forbindelse, at en regulering af den registreredes indsigtsret indgår i det forslag til en databeskyttelsesforordning, som i øjeblikket er under forhandling i EU.

2.4. I forhold til princippet om, *at* medarbejdere hos såvel offentlige myndigheder som private virksomheder udelukkende bør have adgang til de følsomme og fortrolige personoplysninger, som er nødvendige for udførelsen af deres arbejde, *at* det bør sikres, at der løbende føres kontrol hermed, og *at* der generelt bør gælde et *need to know*-princip i forhold til adgang til følsomme og fortrolige personoplysninger, bemærkes det, at det følger af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Bestemmelsen i § 41, stk. 3, er uddybet i bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen). Det følger af bekendtgørelsens § 11, stk. 1, at kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles. Af § 11, stk. 2, følger, at der kun må autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

Sikkerhedsbekendtgørelsen gælder alene for offentlige myndigheder. Der er ikke fastsat uddybende regler om behandlingssikkerhed i den private sektor, hvorfor det er bestemmelsen i persondatalovens § 41, stk. 3, som spørgsmål herom må afgøres efter.

Datatilsynet har imidlertid udtalt, at det er tilsynets opfattelse, at § 41, stk. 3, medfører, at der som udgangspunkt må stilles samme krav til datasikkerheden i den private sektor som i den offentlige forvaltning, og tilsynet anbefaler generelt, at private dataansvarlige i videst muligt omfang tilrettelægger deres sikkerhedsforanstaltninger i overensstemmelse med sikkerhedsbekendtgørelsen.

2.5. For så vidt angår princippet om, at dansk registerforskning er af stor betydning, men at borgernes ret til privatliv og datasikkerhed bør prioriteres, f.eks. gennem anonymisering og pseudonymisering, har Sundheds- og Ældreministeriet oplyst følgende:

> "Udlevering af data, der indeholder personoplysninger om patienters helbredsforhold mv., til brug for forskning på sundhedsområdet, herunder registerforskning, bør som udgangspunkt ikke 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 med øget brug af pseudonymisering af personoplysninger til forskningsprojekter, eksempelvis gennem såkaldte forskermaskine-løsninger.
>
> Sundheds- og Ældreministeriet [støtter] på den baggrund […] en yderligere brug af anonymisering og pseudonymisering. Samtidigt er 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 bidrager til beskyttelsen af individet."

2.6. Hvad angår princippet om, at nødvendigheden af registrering til alle tider bør overvejes, og at man bør stræbe efter mindst mulig registrering, bemærkes det, at det følger af persondatalovens § 5, stk. 3, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles. Det følger desuden af § 5, stk. 5, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere

tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

2.7. Hvad angår 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 bliver prioriteret. Dels er der med aftalerne om fordeling af forskningsreserven i 2014 og i 2015 afsat midler til forskning i cybersikkerhed. Dels er der i National strategi for cyber- og informationssikkerhed tre initiativer vedrørende forskning og uddannelse i cyber- og informationssikkerhed:
>
> - Cyber- og informationssikkerhedsnetværk blandt uddannelses- og forskningsinstitutioner (initiativ 4)
> - Styrket dialog mellem private og offentlige aftagere og de relevante uddannelses- og forskningsinstitutioner (initiativ 5)
> - Nordisk samarbejde om forskning og uddannelse i cyber- og informationssikkerhed (initiativ 20)"

2.8. I forhold til princippet om, *at* der bør være grænser for, hvor indgribende og omfattende et samtykke der kan gives på egne eller andres vegne i forhold til salg og udnyttelse af følsomme og fortrolige persondata, *at* der bør stilles krav om, at politikker om privatlivets fred forklares i et forståeligt sprog, og *at* den registrerede eksplicit samtykker, førend personoplysninger anvendes, har Justitsministeriet indhentet en udtalelse fra Datatilsynet, der har oplyst følgende:

> "For at der foreligger et gyldigt samtykke til behandling af personoplysninger efter persondataloven skal der være tale om en "frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling", jf. persondatalovens § 3, nr. 8.
>
> Heraf følger, at et samtykke skal meddeles i form af en *viljestilkendegivelse* fra den registrerede person. Der er dog intet til hinder for, at et samtykke meddeles af en person, som af den registrerede er meddelt fuldmagt hertil. Der gælder ikke noget formkrav til et samtykke. Der kan således være tale om såvel skriftligt som mundtligt samtykke fra den registrerede.
>
> Et samtykke skal endvidere være *frivilligt*. Samtykket må således ikke være afgivet under tvang.
>
> Herudover skal der være tale om et *specifikt* samtykke. I kravet

herom ligger, at et samtykke skal være konkretiseret i den forstand, at det klart og utvetydigt fremgår, hvad det er, der meddeles samtykke til. Det skal således af et meddelt samtykke fremgå, hvilke typer af oplysninger der må behandles, hvem der kan foretage behandling af oplysninger om den samtykkende, og til hvilke formål behandlingen kan ske.

Endelig skal samtykket være *informeret* i den forstand, at den samtykkende skal være klar over, hvad det er, vedkommende meddeler samtykke til. Den dataansvarlige må således sikre sig, at der gives den registrerede tilstrækkelig information til, at den pågældende kan vurdere, hvorvidt samtykke bør meddeles.

Ud over de ovennævnte krav skal de grundlæggende betingelser i persondatalovens § 5 om saglighed, rimelighed og proportionalitet altid være opfyldt. Et samtykke vil således ikke være tilstrækkeligt til, at en behandling af personoplysninger lovligt kan finde sted. Den dataansvarlige virksomhed eller myndighed skal have et saglig formål med behandlingen, og de personoplysninger, der indsamles og registreres mv., må ikke være irrelevante eller uproportionale i forhold til formålet.

Datatilsynet har eksempelvis udtalt, at det normalt ikke kan anses for sagligt og relevant, at en forretningsdrivende – selv om der foreligger samtykke – registrerer en kundes personnummer, hvis der er tale om et køb, hvor kunden betaler kontant for et produkt, og produktet herefter udleveres, og hvor der herefter ikke er nogen forbindelse mellem kunden og den forretningsdrivende.

For så vidt angår kreditoplysningsbureauer og såkaldte adresserings- og kuverteringsbureauer indeholder persondataloven et forbud mod, at disse virksomheder behandler følsomme oplysninger omfattet af persondatalovens §§ 7 og 8, uanset om der indhentes samtykke fra de registrerede personer."

2.9. I forhold til princippet om, at der bør være en indberetningspligt ved tab af kontrol med følsomme og fortrolige personoplysninger, bemærkes det, at det følger af Datatilsynets praksis vedrørende kravet om god databehandlingsskik i persondatalovens § 5, stk. 1, at der i tilfælde, hvor personoplysninger er kommet til uvedkommendes kendskab eller har været i risiko herfor, som udgangspunkt skal ske underretning af de berørte personer. Der gælder derimod ikke en pligt til at underrette Datatilsynet i sådanne tilfælde.

I forhold til teleområdet har Erhvervs- og Vækstministeriet oplyst følgende:

”Det kan oplyses, at det følger af § 8, stk. 1, og stk. 2, nr. 2, i lov om elektroniske kommunikationsnet og -tjenester (teleloven), at erhvervs- og vækstministeren fastsætter regler for udbydere af offentlige elektroniske kommunikationsnet og -tjenester om minimumskrav til behandling af persondata i elektroniske kommunikationsnet og -tjenester, herunder at der skal ske underretning til Erhvervsstyrelsen ved brud på persondatasikkerheden. Kravet er en implementering af artikel 4.3 i e-Databeskyttelsesdirektivet 2002/58, der blev tilføjet ved den seneste direktivændring i 2009.

Et brud på persondatasikkerheden skal i medfør af det nævnte direktiv forstås som et sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles i forbindelse med udbuddet af offentligt tilgængelige kommunikationstjenester i unionen, jf. artikel 2, litra h, i direktiv 2002/58/EF.

Reglernes anvendelsesområde er afgrænset til udbydere af offentlige elektroniske kommunikationsnet og -tjenester, dvs. i praksis teleselskaberne.

De nærmere regler for underretningspligten og den faste procedure, som skal iagttages, følger af informationssikkerhedsbekendtgørelsen og kommissionens forordning (EU) nr. 613/2013 af 24. juni 2013. Det følger bl.a. heraf, at en udbyder senest 24 timer efter at have påvist et brud på persondatasikkerheden skal underrette Erhvervsstyrelsen herom samt fremsende nærmere angivne oplysninger om bruddet.

Hvis udbyderen ikke har mulighed for at fremskaffe alle de påkrævede oplysninger om bruddet indenfor de første 24 timer, skal udbyderen foretage en indledende underretning til Erhvervsstyrelsen. Denne indledende underretning skal ske senest 24 timer efter påvisningen af bruddet. Udbyderen skal herefter hurtigst muligt og senest tre dage efter den indledende underretning lave en anden underretning til Erhvervsstyrelsen indeholdende de manglende oplysninger om bruddet og om nødvendigt ajourføre de oplysninger, som udbyderen afgav ved den indledende underretning.

Foruden forpligtelsen til at underrette Erhvervsstyrelsen om bruddet på persondatasikkerheden er udbyderen forpligtet til at underrette en abonnent eller fysisk person, hvis bruddet kan forventes at krænke personoplysninger eller privatlivets fred for abonnent eller den fysiske person, medmindre Erhvervsstyrelsen finder det godtgjort, at udbyderen har gennemført passende teknologiske beskyttelsesforanstaltninger, og at disse foranstaltninger er blevet anvendt på de data, som sikkerhedsbruddet vedrørte.

> Underretningerne om brud på persondatasikkerheden til Erhvervsstyrelsen skal ske via et elektronisk format, der findes på den fællesoffentlige indberetningsportal virk.dk."

I det forslag til en databeskyttelsesforordning, som er omtalt under pkt. 1.4 ovenfor, indgår i øvrigt regler om underretningspligt i tilfælde af brud på datasikkerheden. Det følger således af forslaget, at den dataansvarlige uden unødig forsinkelse og – om muligt – senest 72 timer efter, at den dataansvarlige er blevet bekendt med et brud på persondatasikkerheden, skal anmelde bruddet til den kompetente tilsynsmyndighed, medmindre det er usandsynligt, at bruddet vil medføre en risiko for den registreredes rettigheder eller frihedsrettigheder.

Det følger desuden af forslaget, at når sikkerhedsbruddet kan forventes at medføre en høj grad af risiko for den registreredes rettigheder og frihedsrettigheder, skal den dataansvarlige ligeledes uden unødig forsinkelse underrette den registrerede om bruddet.

Forslaget indeholder visse undtagelser til udgangspunktet om underretningspligt.

2.10. Hvad angår princippet om, at lovgivningsinitiativer bør være teknologineutrale, bemærkes det, at de generelle regler om behandling af personoplysninger i persondataloven er teknologineutrale. Lovens regler finder således anvendelse på enhver form for behandling af personoplysninger, der falder inden for lovens anvendelsesområde. Justitsministeriet er i øvrigt generelt enig i, at lovgivningsinitiativer – så vidt muligt – bør være teknologineutrale.

2.11. Hvad angår det sidste princip i beretningen om, at anvendelsen af personoplysninger samt konsekvenser for privatlivets fred – herunder hvordan negative konsekvenser for privatlivets fred kan undgås – bør fremgå af bemærkninger til fremsatte lovforslag, bemærkes det, at det er et helt centralt lovkvalitetskrav, at bemærkningerne til et lovforslag affattes fyldestgørende og korrekt, jf. Justitsministeriets Vejledning om Lovkvalitet (2005), side 13.

Det betyder bl.a., at et fagministerium i de tilfælde, hvor et lovforslag giver anledning til mere omfattende overvejelser i forhold til f.eks. grundloven, EU-retten, Den Europæiske Menneskerettighedskonvention eller al-

mindelige retsprincipper, bør redegøre for disse overvejelser i lovforslagets almindelige bemærkninger, jf. vejledningen, side 23.

Det betyder ligeledes, at lovforslagets specielle bemærkninger normalt bør indeholde oplysning om indholdet af de hidtil gældende regler, om de ændringer heri, som lovforslaget vil medføre, om begrundelsen herfor samt eventuelt om de virkninger, som den foreslåede ændring kan forventes at få, jf. vejledningen, s. 24.

Det anførte gælder også, når lovforslaget vedrører anvendelsen af personoplysninger.

Princippet om, at anvendelsen af personoplysninger samt konsekvenser for privatlivets fred bør fremgå af bemærkningerne til fremsatte lovforslag, kan således allerede anses for indeholdt i Justitsministeriets Vejledning om Lovkvalitet.

3.1. Beretningens afsnit 3.2 indeholder en række anbefalinger og opfordringer vedrørende tilsynet med overholdelse af persondataloven.

Arbejdsgruppen anbefaler bl.a., at det bør overvejes, hvorvidt Datatilsynets kontrolbesøg skal være risikobaserede. Datatilsynet har hertil bemærket følgende:

> ”Datatilsynet har i 2012 udarbejdet en inspektionsstrategi, der fastlægger rammerne for tilsynets inspektionsindsats for 2013-2015.
>
> Det primære formål med Datatilsynets inspektioner er at foretage konkret kontrol hos de inspicerede virksomheder og myndigheder og om nødvendigt at sikre en bedre overholdelse af loven hos virksomheden eller myndigheden.
>
> Som led i strategien har Datatilsynet derfor udvalgt kategorier af virksomheder, myndigheder og databehandlinger, hvor tilsynet vurderer, at der er særligt behov for tilsyn.
>
> Ved udvælgelsen er det navnlig tillagt vægt, at der foregår behandling af store mængder fortrolige eller følsomme personoplysninger. Der er endvidere lagt vægt på, at det for visse former for databehandlinger gælder, at de registrerede personers rettigheder – eksempelvis retten til indsigt – er begrænset på grund af tungtvejende hensyn til bl.a. forebyggelse og efterforskning af straffesager.

Datatilsynet arbejder således allerede med en risikobaseret tilgang til sin inspektionsindsats.

Det indgår imidlertid tillige i tilsynets vurdering, at der i forhold til visse typer af databehandlinger fra politisk side tidligere har været tilkendegivelser om, at der bør føres et aktivt tilsyn. Det gælder eksempelvis tv-overvågningsområdet. I tilsynets inspektionsaktiviteter indgår også koordinerede indsatser, som besluttes på EU-niveau i de fælles tilsynsmyndigheder inden for eksempelvis Schengen-samarbejdet.

Endelig må det ved planlægning af inspektionsindsatsen vurderes, hvad der realistisk set er mulighed for, at sætte fokus på med de forhåndenværende ressourcer.

I den forbindelse bemærkes, at Datatilsynet har inspektionskompetence i forhold til den offentlige forvaltning, dvs. de statslige, kommunale og regionale myndigheder.

I forhold til den private sektor har Datatilsynet som udgangspunkt adgang til at foretage inspektioner, når der er anmeldelsespligt til tilsynet. Der er aktuelt over 10.000 anmeldte behandlinger fra private dataansvarlige, som hermed er underlagt Datatilsynets inspektionskompetence.

Herudover har tilsynet inspektionskompetence over for private dataansvarlige, der foretager behandlinger af personoplysninger i forbindelse med tv-overvågning. Inspektioner på tv-overvågningsområdet har udgjort en markant del af tilsynets inspektionsvirksomhed i de seneste år."

3.2. Det anbefales desuden i beretningen, at der iværksættes en undersøgelse af, hvordan man kan styrke den tværfaglige videnopsamling og rådgivning af offentlige institutioner og private virksomheder.

Som nævnt vil regeringen på baggrund af den under punkt 1.3 ovenfor nævnte politiske drøftelse udarbejde en samlet strategi til sikring af danskernes personoplysninger. Spørgsmålet om tværfaglig videnopsamling og rådgivning af offentlige institutioner og private virksomheder vil være et af de emner, der vil skulle ses nærmere på i den forbindelse.

Det kan desuden oplyses, at der som led i en opprioritering af databeskyttelsesområdet er blevet oprettet et nyt Databeskyttelseskontor, der navnlig vil få ansvaret for persondatalovgivningen. Kontoret har bl.a. ansvaret for rådgivning af andre ministerier om persondataretlige spørgsmål, koordination af regeringens politik på området og for at repræsentere Danmark i diverse internationale fora, hvor persondatabeskyttelse behandles.

Der henvises i øvrigt til pkt. 2.2 ovenfor om Datatilsynets rådgivning og vejledning.

3.3. Det anbefales herudover, at det overvejes, om der bør etableres en klageinstans til at behandles klager over Datatilsynets afgørelser.

Det bemærkes hertil, at Datatilsynet består af et råd – benævnt Datarådet – og et sekretariat. Datarådet består af en formand og 6 andre medlemmer, der er udpeget af justitsministeren. Datarådet fastsætter selv sin forretningsorden.

Af Datarådets forretningsordenen fremgår bl.a., at rådet behandler og træffer afgørelse i sager 1) af principiel karakter, 2) af betydelig almindelig interesse eller med betydelige følger for en offentlig myndighed eller privat virksomhed m.v., 3) der af andre særlige grunde findes at burde afgøres af rådet, og 4) som et rådsmedlem ønsker optaget til rådsbehandling.

Som nævnt i Justitsministeriets besvarelse af 30. oktober 2014 af spørgsmål nr. 1604 (Alm. del) fra Retsudvalget fremgår det ikke direkte af det nugældende databeskyttelsesdirektiv, om der inden for de rammer, der følger af direktivet, kan etableres en almindelig klageinstans til at behandle klager over Datatilsynets afgørelser. Det er imidlertid Justitsministeriets umiddelbare vurdering, at direktivet ikke generelt er til hinder for etablering af en sådan ordning.

Som det også fremgår af den nævnte besvarelse, indeholder det forslag til en generel databeskyttelsesforordning, som i øjeblikket forhandles i EU, regler om uafhængige tilsynsmyndigheder. Forordningsforslaget indeholder – i forhold til de tilsvarende regler i det gældende databeskyttelsesdirektiv – mere detaljerede krav til de nationale tilsynsmyndigheders organisering og uafhængighed.

Det er på den baggrund Justitsministeriets opfattelse, at den nærmere indretning af tilsynssystemet på databeskyttelsesområdet bør afvente den kommende databeskyttelsesforordning.

Datatilsynet har om spørgsmålet om etablering af en klageinstans i øvrigt bemærket følgende:

> ”Datatilsynsmyndighederne i EU er organiseret på forskellig vis. Den danske model med et råd og et sekretariat findes så vidt vides ikke i andre EU-lande.
>
> I forbindelse med persondatalovens tilblivelse blev det drøftet, om der skulle etableres en ordning med et ankenævn, eller om registerlovenes ordning med et råd skulle videreføres. Registertilsynets repræsentant i det lovforberedende udvalg indgik i det flertal, der støttede den nuværende model. Der henvises herved til forarbejderne til persondataloven.
>
> Af de i forarbejderne anførte grunde er det fortsat tilsynets opfattelse, at en ordning med etablering af et klageorgan i forhold til Datatilsynet er unødvendig og vil være uhensigtsmæssig.
>
> Den norske model med et klagenævn er tilsynet bekendt heller ikke meget udbredt. Flere lande har en databeskyttelseskommissær eller eventuelt en kommission bestående af flere kommissærer.
>
> I Sverige havde Datainspektionen frem til januar 2008 et råd (styrelse). Dette er imidlertid blevet erstattet af et såkaldt ”insynsråd”, som skal følge tilsynets arbejde, som nu ledes af generaldirektøren.”

4. Beretningens afsnit 3.3 indeholder anbefalinger og opfordringer vedrørende sanktionsmuligheder ved brud på datasikkerhed.

Det anføres bl.a., at arbejdsgruppen er enig om, at Datatilsynets nuværende sanktionsmuligheder ikke er tilstrækkelige, og at der er behov for, at yderligere sanktionsmuligheder indføres. Arbejdsgruppen opfordrer desuden til, at det undersøges, om anvendelsesområdet for de nuværende straffebestemmelser på området er tilstrækkeligt dækkende, samt om strafniveauet er tilstrækkeligt.

Særligt for så vidt angår spørgsmålet om at tillægge Datatilsynet mulighed for at udstede administrative bøder, kan der henvises til Justitsministeriets besvarelse af 7. november 2014 af spørgsmål nr. 1605 (Alm. del) fra Folketingets Retsudvalg. Som det fremgår heraf, ville en sådan ordning indebære grundlovsmæssige betænkeligheder.

Spørgsmålet om Datatilsynets sanktionsmuligheder bør efter Justitsministeriets opfattelse i øvrigt henskydes til den under pkt. 1.3 ovenfor nævnte politiske drøftelse.

I forhold til arbejdsgruppens opfordring til, at offentlige myndigheder og private virksomheder bør gøres til genstand for samme sanktionsmuligheder, bemærkes det, at persondatalovens § 70 indeholder bestemmelser om strafansvar for overtrædelse af lovens regler. Bestemmelsen sondrer mellem, om behandlingen udføres for private eller for offentlige myndigheder. Overtrædelse af reglerne om behandling af personoplysninger, som udføres for private, er i langt videre omfang strafbelagt end overtrædelse af reglerne om behandlinger, som udføres for offentlige myndigheder.

Det fremgår af forarbejderne til persondataloven, at baggrunden for, at der gælder separate straffebestemmelser for behandling af personoplysninger, der udføres for henholdsvis private og for offentlige myndigheder, bl.a. er, at man havde en tilsvarende ordning i de tidligere gældende registerlove, idet der i bl.a. straffeloven er fastsat en række bestemmelser om tjenesteansvar for personer i offentlig tjeneste eller hverv mv. (se kapitel 16 om forbrydelser i offentlig tjeneste eller hverv mv., herunder §§ 152-152 f om tavshedspligt), ligesom der også er mulighed for at pålægge offentligt ansatte et disciplinært ansvar (jf. betænkning nr. 1345/1997 om behandling af personoplysninger, s. 389).

Det bemærkes, at overtrædelse af persondataloven kan begås af både fysiske og juridiske personer, herunder offentlige myndigheder, hvis de generelle betingelser herfor er opfyldt, jf. nedenfor.

Strafansvaret for offentlige myndigheder som sådan er imidlertid undergivet den begrænsning, der følger af den generelle bestemmelse i straffelovens § 27, stk. 2. Efter denne bestemmelse kan statslige myndigheder og kommuner alene straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private.

Som argumenter mod strafansvar for offentlige myndigheder er det generelt bl.a. blevet anført, *at* en bøde til en statslig myndighed kan siges at være uden præventiv værdi, idet bøden tilfalder statskassen, *at* offentlige myndigheder i modsætning til den private sektor ved grundloven og lovgivningen i øvrigt er pålagt at udføre bestemte opgaver, og at en myndighed derfor ikke uden videre blot kan standse sin virksomhed for derved straks at bringe en eventuel ulovlig tilstand til ophør, *at* de bevillingsretlige regler indebærer, at en myndighed ikke uden videre kan skaffe midler til at afhjælpe en ulovlig tilstand, hvis der ikke er mulighed herfor inden for de økonomiske rammer, der er stillet til rådighed, samt *at* der inden for den

offentlige sektor gælder særlige regler om fordeling af ansvar, ligesom det er en tjenestepligt at overholde retsregler, herunder også regler der er strafferetligt sanktioneret, jf. Straffelovrådets betænkning nr. 1289/1995 om juridiske personers bødeansvar, side 69.

Når statslige myndigheder og kommuner ikke desto mindre kan straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, som svarer til eller kan sidestilles med virksomhed udøvet af private, skyldes det hensynet til i henseende til straf at ligestille offentlige myndigheder med private aktieselskaber mv., når myndighederne udøver virksomhed af samme art. Det ville således være utilfredsstillende, hvis en offentlig myndighed kunne overtræde lovgivningen og gå fri for straf i tilfælde, hvor en tilsvarende overtrædelse begået af en privat virksomhed ville medføre strafansvar. Der henvises til Straffelovrådets betænkning nr. 1289/1995 om juridiske personers bødeansvar, side 69-70.

Justitsministeriet finder på den baggrund ikke, at offentlige myndigheder og private virksomheder bør gøres til genstand for samme sanktionsmuligheder.

5. Beretningens afsnit 3.4 indeholder opfordringer vedrørende samling af ansvaret for datasikkerhed.

Det bemærkes hertil, at spørgsmål om adgangen til at behandle personoplysninger er reguleret i både de generelle regler i persondataloven og en række særlige regler i den øvrige lovgivning, f.eks. lovgivningen på sundhedsområdet og det finansielle område.

Det følger i den forbindelse af persondatalovens § 2, stk. 1, at regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i persondataloven. Omvendt følger det af bestemmelsen, at loven finder anvendelse, hvis regler om behandling af personoplysninger i anden lovgivning giver den registrerede en dårligere retsstilling. Dette gælder ifølge lovens forarbejder dog ikke, hvis den dårligere retsstilling har været tilsigtet og i øvrigt ikke strider mod databeskyttelsesdirektivet.

Det er regeringens opfattelse, at det er mest hensigtsmæssigt, at der på særlige områder, f.eks. sundhedsområdet eller det finansielle område, kan ske en regulering af adgangen til at behandle personoplysninger, som enten udvider eller indskrænker den beskyttelse, der følger af de generelle regler

i persondataloven. Det er desuden regeringens opfattelse, at en sådan regulering mest naturligt hører under den minister, som har ansvaret for og den største ekspertise til rådighed vedrørende det område, der reguleres.

Som nævnt ovenfor under pkt. 3.2 er der i øvrigt i Justitsministeriet blevet oprettet et nyt Databeskyttelseskontor, der navnlig har ansvaret for persondatalovgivningen.

6.1. Beretningens afsnit 3.5 indeholder en række anbefalinger og opfordringer vedrørende tekniske krav til sikring af følsomme og fortrolige personoplysninger.

6.2. I forhold til anbefalingerne vedrørende implementering af *privacy by design* har Finansministeriet bemærket følgende:

> "Finansministeriet er enig med arbejdsgruppen i, at hensynet til borgernes privatliv er et væsentligt princip, når it-systemer udvikles og designes. Netop derfor er der i den nationale strategi for cyber- og informationssikkerhed indskrevet i initiativ 2, at de statslige myndigheder som grundlæggende præmis skal arbejde med privatlivsbeskyttelse, jf. overvejelserne bag "privacy-by-design" ved nyudvikling af nye it-projekter. Ligeledes fremgår det i samme initiativ, at der i 2015 skal indarbejdes krav om en privatlivsrelateret og sikkerhedsmæssig risikovurdering i Statens It-projektmodel.
>
> Finansministeriet er optaget af at sikre, at både nye og gamle it-systemer har et passende sikkerhedsniveau, men finder, at et krav med tilbagevirkende kraft om at ændre eksisterende it-systemer, så de lever op til principperne bag privacy-by-design vil være særdeles omkostningstungt. Ældre systemer er generelt set konstrueret med sikkerhedsmodeller, der ikke lever op til principperne bag privacy-by-design, men er løbende tilpasset tidens sikkerhedsudfordringer. Det kan derfor blive særdeles omkostningsfuldt at skulle tilpasse alle disse systemer, så de lever op til principperne bag privacy-by-design."

6.3. I forhold til anbefalingerne vedrørende sikkerhedsstandarden ISO27001 har Finansministeriet bemærket følgende:

> "Finansministeriet noterer sig, at arbejdsgruppen støtter op om implementeringen af ISO27001. For at sikre en hurtig overgang til den nye standard, er det i strategien for cyber- og informationssikkerhed blevet fastlagt, at alle statslige myndigheder skal have implementeret standarden primo 2016.

> Finansministeriet vurderer, at det ikke er praktisk muligt, at alle statslige myndigheder har gennemført implementeringen af ISO27001 hurtigere end det i strategien fastlagte tidspunkt."

6.4. I forhold til anbefalingerne vedrørende kontrol af rollebaseret adgang bemærkes det, at det følger af den under pkt. 2.4 ovenfor nævnte sikkerhedsbekendtgørelses § 17, stk. 1 og 2, at det skal sikres, at autoriserede personer fortsat opfylder betingelserne i § 11, stk. 2 og 3, og § 16 for at være autoriserede, og at kontrol heraf skal foretages mindst en gang hvert halve år.

Finansministeriet har i forhold til anbefalingerne vedrørende kontrol af rollebaseret adgang bemærket følgende:

> "Som følge af initiativ 7 i cyber- og informationssikkerhedsstrategien vil Digitaliseringsstyrelsen sikre en systematisk erfaringsudveksling af sikkerhedsmæssige krav mellem relevante myndigheder, der udbyder og indgår kontrakter på it-området. Endvidere vil styrelsen udarbejde en liste over sikkerhedsmæssige krav, som myndighederne kan bruge som inspiration i arbejdet med it-driftskontrakter. I forbindelse med dette arbejde vil styrelsen udarbejde sikkerhedsmæssige standardklausuler, som kan benyttes i it-driftskontrakter. I den forbindelse vil styrelsen vurdere behovet for særskilte standardklausuler om kontrol med brugeradgange."

7.1. Beretningen indeholder endelig i afsnit 3.6 en række øvrige bemærkninger.

7.2. Arbejdsgruppen anbefaler bl.a., at der igangsættes en udredning af, om der bør være grænser for, hvad der kan samtykkes til, og i så fald, hvor grænserne for samtykke bør drages.

Det bemærkes hertil, at der som nævnt for tiden pågår forhandlinger i EU-regi om en forordning på databeskyttelsesområdet, som skal erstatte det nugældende databeskyttelsesdirektiv. Der lægges med forordningsforslaget op til at regulere kravene til et samtykke til behandling af personoplysninger. På den baggrund finder Justitsministeriet det ikke hensigtsmæssigt at iværksætte en udredning som den foreslåede på nuværende tidspunkt.

Der henvises i øvrigt til det ovenfor under pkt. 2.8 anførte.

7.3. Det anbefales desuden, at der foretages en kortlægning af eksisterende offentlige registre, og at det i den forbindelse bør overvejes, om der i nogle

tilfælde registreres og opbevares mere data end nødvendigt.

Justitsministeriet bemærker hertil, at arbejdet med en sådan kortlægning må antages at være endog særdeles ressourcekrævende.

Hertil kommer, at det følger af persondatalovens § 5, stk. 4, at behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne, og at der skal foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Der påhviler således den enkelte dataansvarlige myndighed eller virksomhed mv. en forpligtelse til om nødvendigt at foretage kontrol med og ajourføring af oplysninger.

Justitsministeriet har på den baggrund ikke planer om at iværksætte en kortlægning som den foreslåede.

7.4. I forhold til anbefalingen om, at der udarbejdes en national strategi for informations- og datasikkerhed for den samlede offentlige sektor, bemærkes, at den kortlægning af beskyttelsen af oplysninger om borgernes elektroniske betalinger mv., som den tidligere justitsminister bad sine embedsmænd om at foretage sammen med Erhvervs- og Vækstministeriet (og andre relevante ministerier), som nævnt vil skulle danne udgangspunkt for en politisk drøftelse. Regeringen vil på baggrund af den politiske drøftelse som nævnt udarbejde en samlet strategi til sikring af danskernes personoplysninger.

Finansministeriet har i forhold til anbefalingen om udarbejdelse af en national strategi for informations- og datasikkerhed bemærket følgende:

> ”Finansministeriet er enig i, at der skal arbejdes ensartet og systematisk med sikkerhed på tværs af hele den offentlige sektor. Regeringen, KL og Danske Regioner har i forbindelse med de årlige økonomiaftaler aftalt, at arbejdet med informationssikkerhed skal styrkes yderligere med henblik på at sikre fortrolighed om personfølsomme oplysninger og et højt sikkerhedsniveau i den digitale infrastruktur. Dette samarbejde forventes styrket i den kommende Digitaliseringsstrategi, der udarbejdes i samarbejde mellem staten, kommunerne og regionerne og forventes lanceret primo 2016.
>
> Yderligere fremgår det af cyber- og informationssikkerhedsstrategien, at Digitaliseringsstyrelsen sammen med de fællesoffentlige parter vil vurdere, om der i staten, kommuner og regioner er behov for yderligere indsats i forhold til implemente-

ring af ISO27001, når effekterne af initiativerne fra strategien kan vurderes."

7.5. I forhold til det af arbejdsgruppen anførte om, at brugen af cpr-nummeret bør gennemgå en grundlæggende revidering, har social- og indenrigsministeren bemærket følgende:

"Det er ikke min opfattelse, at der er behov for, at det nuværende personnummersystem afvikles eller revideres.

Personnummeret er en ti-cifret kode, som tjener til entydigt at identificere en person, f.eks. i et it-system. Det er personnummeret ganske effektivt til. 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 hjælp af NemID, 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. Det kan tilføjes, at Social- og Indenrigsministeriet i dag stiller krav om anvendelse af NemID i forbindelse med virksomheders og myndigheders selvbetjeningsløsninger, hvorfra der foretages opslag i CPR.

Det bemærkes i den forbindelse, at det fremgår af justitsministerens besvarelse af spørgsmål 1305 (Alm. del) af 23. januar 2015 fra Folketingets Retsudvalg, at Rigspolitiet har oplyst, at politiet tidligere modtog en del anmeldelser om svindel på internettet ved brug af CPR-nummer som eneste autentifikation ved nethandel, herunder særligt ved køb af mobiltelefoner og tablets hos teleudbydere eller optagelse af såkaldte ekspres- eller mikrolån hos finansieringsselskaber.

Det fremgår også af besvarelsen, at Rigspolitiet har oplyst, at teleudbydere, finansieringsselskaber og andre handlende på internettet dog i dag næsten altid stiller krav om anvendelse af NemID som autentifikation, og at politiet i dag kun sjældent modtager anmeldelser om svindel på internettet, hvor et CPR-nummer er anvendt som eneste grundlag for autentifikation. Det fremgår af besvarelsen af spørgsmålet, at det på den baggrund er Rigspolitiets vurdering, at bl.a. udbredelsen af NemID som middel til autentifikation har nedbragt risikoen for identitetsmisbrug.

Det er derfor også positivt, at Social- og Indenrigsministeriet på nuværende tidspunkt alene har modtaget 33 ansøgninger om nyt personnummer som følge af identitetsmisbrug, hvori personnummeret indgår.

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.

Det kan tilføjes, at Datatilsynet har gennemført en egen driftundersøgelse af den hændelse, som omtales i udvalgets beretning, hvor 900.000 personnumre på en lukket del af CPR-kontorets hjemmeside var tilgængelig for virksomheder i ca. 50 minutter. Datatilsynet har ved brev af 15. maj 2015 udtalt følgende:

"I det konkrete tilfælde, hvor et meget stort antal personnumre blev gjort tilgængelige for uvedkommende sammen med navne og adresser, finder Datatilsynet det skete meget kritisabelt.

Datatilsynet skal herved henvise til, at offentliggørelse af oplysninger om personnummer i kombination med navn og adresse i værste fald ville kunne få alvorlige konsekvenser for en berørt person.

Det er endvidere Datatilsynets opfattelse, at der navnlig i situationer, hvor der er en potentiel risiko for offentliggørelse af fortrolige og/eller følsomme personoplysninger, skal udvises særlig påpasselighed, både for så vidt angår tilrettelæggelsen af arbejdsgange og for så vidt angår indretningen af myndighedens systemer.

Datatilsynet har i øvrigt noteret sig det af CPR-kontoret oplyste om:

- *at listen blev fjernet fra cpr.dk umiddelbart efter, at CPR-kontoret blev bekendt med, at listen indeholdt oplysninger om personnumre,*
- *at CPR-kontoret i sine logfiler har kunnet konstatere, at listen er downloadet maksimalt 18 gange,*
- *at CPR-kontoret rettede henvendelse til alle de virksomheder, som kontoret umiddelbart kunne konstatere havde downloadet listen, og meddelte, at listen skulle destrueres,*
- *at CPR-kontoret kontaktede virksomheder tilmeldt nyhedsbrevet om opdateringer af Robinson-listen og meddelte, at virksomheder, der havde downloadet listen, skulle destruere denne og give CPR-kontoret skriftlig meddelelse derom,*

- *at CPR-kontoret efterfølgende har modtaget bekræftelse på, at alle downloadede lister i forbindelse med sikkerhedshændelsen er blevet destrueret,*
- *at CPR-kontoret ved søgninger på internettet ikke har kunnet konstatere, at den pågældende fil er tilgængelig, samt*
- *at CPR-kontoret løbende holder øje hermed med henblik på i givet fald straks at fjerne oplysningerne fra eventuelle hjemmesider, og at Center for Cybersikkerhed støtter CPR kontoret i denne proces.*

Endelig har Datatilsynet noteret sig det oplyste om:

- *at CPR-kontoret har offentliggjort en pressemeddelelse med sammenfattende oplysninger til borgerne om sikkerhedshændelsen,*
- *at CPR-kontoret som følge af sikkerhedshændelsen umiddelbart har indført en intern procedure med dobbeltkontrol af Robinson-listen, før denne lægges på cpr.dk.*
- *at CPR-kontoret er i dialog med CSC Danmark A/S om passende sikkerhedsforanstaltninger, samt*
- *at interne retningslinjer og forretningsgange vedrørende produktion og levering af Robinson-listen vil blive revideret med henblik på at undgå, at situationen gentager sig."*

Social- og Indenrigsministeriet har taget Datatilsynets udtalelse til efterretning. Som det fremgår af udtalelsen, har CPR-kontoret truffet foranstaltninger for at undgå, at en sådan meget beklagelig situation gentager sig."

8. Jeg ser frem til den politiske drøftelse om databeskyttelse med Folketingets politiske partier og til arbejdet med at udarbejde en samlet strategi til sikring af danskernes personoplysninger.