FOLKETINGSTIDENDE B

FOLKETINGET

Beretning nr. **4** Folketinget 2014-15

Beretning afgivet af Retsudvalget den 15. januar 2015

Beretning

om datasikkerhed

1. Indledning

Folketingets Retsudvalg afgiver på baggrund af indstilling fra arbejdsgruppen om datasikkerhed hermed nærværende beretning.

Kulturudvalget og Retsudvalget konkluderede på baggrund af Se og Hør-sagen i foråret 2014, at sagen vidnede om et generelt behov for bedre datasikkerhed og en mere restriktiv kontrolindsats med behandlingen af følsomme og fortrolige personoplysninger.

Kulturudvalget og Retsudvalget afgav den 3. juni 2014 en fælles beretning om nedsættelse af en parlamentarisk arbejdsgruppe, der skulle undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med offentlige institutioner såvel som private virksomheders behandling af disse, jf. beretning nr. 3 af 3. juni 2014 (REU alm. del – bilag 289, folketingsåret 2013-14).

På baggrund af beretningen blev der nedsat to parlamentariske arbejdsgrupper: arbejdsgruppen om datasikkerhed under Retsudvalget og arbejdsgruppen om medieetik og medieansvar under Kulturudvalget. Arbejdsgruppen om datasikkerhed blev nedsat med en repræsentant for hver partigruppe og udgjorde således 8 medlemmer. Se og Hør-sagen blev betragtet som en aktualisering af en generel problemstilling angående datasikkerhed, og arbejdsgruppen om datasikkerhed blev derfor nedsat med det formål at foretage en bred afdækning af beskyttelsen af borgernes følsomme og fortrolige personoplysninger.

Siden arbejdsgruppen blev nedsat, er der foretaget flere kortlægninger af problemstillinger på datasikkerhedsområdet. Såvel Rigsrevisionens »Beretning om statens behandling af fortrolige oplysninger om personer og virksomheder« som Digitaliseringsstyrelsens og Center for Cybersikkerheds »Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift« har understreget behovet for en indsats i forhold til at højne datasikkerheden.

Også den kommende EU-forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) har sat fokus på datasikkerhed og arbejdsgruppen har med interesse fulgt de igangværende forhandlinger. Det nuværende forordningsforslag indeholder positive initiativer, og arbejdsgruppen afventer, at der foreligger et endeligt forordningsforslag. Arbejdsgruppen er af den generelle opfattelse, at Danmark allerede nu bør påbegynde arbejdet med at gennemføre de dele af forordningen, der på nuværende tidspunkt er enighed om.

Arbejdsgruppen har koncentreret arbejdet om en række af de i beretning nr. 3 nævnte områder og ud fra disse søgt at identificere problemstillinger og løsningsmuligheder for i nærværende beretning at fremlægge principielle overvejelser samt fremsætte en række anbefalinger.

På baggrund af arbejdsgruppens ressourcer har arbejdsgruppen valgt at fokusere på følgende områder:

- Principper for datasikkerhed.
- Tilsynet med overholdelsen af persondataloven.
- Sanktionsmuligheder ved brud på datasikkerhed og manglende overholdelse af gældende lov.
- Samling af ansvaret for datasikkerhed.
- Tekniske krav til sikring af følsomme og fortrolige personoplysninger.

Arbejdsgruppen ønsker dog at understrege, at der også eksisterer en række datasikkerhedsudfordringer og dilemmaer i forhold til sociale medier, overvågningskameraer, spionageparagrafferme og logningsregler, som arbejdsgruppen håber at partigrupperne ved en anden lejlighed vil diskutere. I forhold til logningsregler noterer arbejdsgruppen sig, at det fremgår af regeringens lovprogram for folketingsåret 2014-15, at justitsministeren har til hensigt at fremsætte et forslag om revision af de gældende logningsregler i februar 2015. Arbejdsgruppen ser frem til den debat, lovforslaget vil give anledning til.

Beretningen er baseret på de initiativer, arbejdsgruppen har taget siden sommeren 2014, herunder en skriftlig høring, mundtlige høringer, møder med tekniske og juridiske eksperter m.v. Arbejdsgruppen har yderligere stillet en række spørgsmål til andre europæiske lande bl.a. om de respektive landes datatilsyn og datasikkerhedsproblematikker samt

kontaktet en række applikationsudbydere angående deres adgang til applikationsbrugernes oplysninger.

Arbejdsgruppen noterer sig, at regeringen er enig i, at der er behov for at undersøge nye initiativer i forhold til beskyttelse af personoplysninger, jf. REU alm. del – svar på spørgsmål 1240, folketingsåret 2013-14. Videre finder arbejdsgruppen det positivt, at justitsministeren har udvist velvilje i forhold til arbejdsgruppens arbejde, herunder at justitsministeren har indkaldt til en politisk drøftelse om styrkelse af Datatilsynet, om afgivelse af en årlig redegørelse til Folketinget om datasikkerhed og generelt om de overvejelser, som arbejdet i arbejdsgruppen måtte give anledning, jf. REU alm. del – svar på spørgsmål 1240, folketingsåret 2013-14.

Datasikkerhed og beskyttelse af borgernes følsomme og fortrolige data er en voksende bekymring, der deles af såvel Folketing som regering, og som går på tværs af partierne i Folketinget. Arbejdsgruppen ser derfor frem til et konstruktivt samarbejde om at øge datasikkerheden.

2. Arbejdsgruppens arbejde

Medlemmer

Arbejdsgruppen bestod af: Karsten Lauritzen, fmd. (V), Dennis Flydtkjær (DF), Tom Behnke (KF), Simon Emil Ammitzbøll (LA), Trine Bramsen (S), Jeppe Mikkelsen (RV), Karina Lorentzen Dehnhardt (SF) og Pernille Skipper (EL).

Møder

Arbejdsgruppen har afholdt 11 møder, herunder et dialogmøde med Forbrugerombudsmanden, Forbrugerrådet Tænk, Institut for Menneskerettigheder, Rådet for Digital Sikkerhed og Teknologirådet, samt møder med advokat Janne Glæsel, repræsentanter for Datatilsynet og professor Peter Blume.

Høringer

Arbejdsgruppen har afholdt en åben høring den 22. oktober 2014 om offentlige myndigheders behandling af personoplysninger og en åben høring den 12. november 2014 om tekniske tiltag til sikring af følsomme personoplysninger.

Besøg

Arbejdsgruppen har besøgt IBM og TDC.

Spørgsmål

Arbejdsgruppen har stillet 10 spørgsmål til justitsministeren til skriftlig besvarelse, som denne har besvaret.

Arbejdsgruppen har stillet spørgsmål vedrørende datasikkerhed til parlamenterne i henholdsvis Norge, Sverige, Storbritannien og Tyskland gennem det europæiske parlamentssamarbejde, the European Center for Parliamentary Research and Documentation (ECPRD).

Yderligere har arbejdsgruppen kontaktet en række applikationsudbydere angående indsamling af brugerdata. Arbejdsgruppen har modtaget svar fra Danske Bank, DMI, e-Boks, Nordea og Facebook.

Skriftlig høring

Beretning nr. 3 af 3. juni 2014 blev sendt i høring den 2. juli 2014, og arbejdsgruppen modtog 30 høringssvar.

En oversigt over bilag, herunder materiale fra høringer og møder samt spørgsmål og svar, som har relevans for beretningen, er optrykt som bilag 1.

3. Politiske bemærkninger

3.1 Overordnede principper for datasikkerhed

Arbejdsgruppen har på baggrund af arbejdet opstillet en række principper, som arbejdsgruppen mener bør være grundlæggende for it- og dataarbejde.

- Såvel offentlige myndigheder som private virksomheder, der behandler følsomme og fortrolige personoplysninger, bør være sig sit særlige ansvar bevidst. Jo mere følsomme og fortrolige oplysninger, der lagres og behandles, desto større krav på sikkerhed og beskyttelse bør borgeren have.
- Den dataansvarlige bør altid have ansvaret for sikkerheden omkring de følsomme og fortrolige personoplysninger, også når data behandles af en tredjepart. Den dataansvarlige bør altid have ansvaret for, at der stilles tilstrækkelige krav til databehandler ved behandling af følsomme og fortrolige personoplysninger.
- Ud over den dataansvarlige bør også databehandleren selvstændigt kunne gøres ansvarlig for overholdelse af reglerne om databeskyttelse.
- Myndigheder, der fører tilsyn med datasikkerhed, bør være stærke og uafhængige. Tilsynsmyndighederne bør have tilstrækkelige ressourcer og kompetencer samt prioritere kontrolbesøg.
- Virksomheder og offentlige myndigheder bør have adgang til vejledning om lovgivning og regulering på databeskyttelsesområdet.
- 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. Dette bør til enhver tid være gældende, medmindre stærke hensyn taler imod.
- Borgere bør til enhver tid have mulighed for at klage, hvis borgeren mistænker en myndighed eller virksomhed for uretmæssigt at opbevare data.
- Medarbejdere hos såvel offentlige myndigheder som private virksomheder bør udelukkende have adgang til de følsomme og fortrolige personoplysninger, som er nødvendige for udførelsen af deres arbejde, og det bør sikres, at der løbende føres kontrol hermed. Der bør generelt gælde et need to know-princip i forhold til adgang til følsomme og fortrolige personoplysninger.
- Nødvendigheden af registrering bør til alle tider overvejes, og man bør stræbe efter mindst mulig registrering.
- Dansk registerforskning er af stor betydning, men borgernes ret til privatliv og datasikkerhed bør prioriteres, f.eks. gennem anonymisering og pseudonymisering.
- Ved samkøring af registre, der indeholder følsomme og fortrolige personoplysninger, bør der tages højde for borgernes retssikkerhed.

- Forskning i datasikkerhed og kryptering bør prioriteres.
- 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. Der bør stilles krav om, at politikker om privatlivets fred forklares i et forståeligt sprog, og at den registrerede eksplicit samtykker, førend personoplysninger anvendes.
- Misbrug af følsomme og fortrolige personoplysninger bør straffes.
- Der bør være en instans, som følger op datasikkerhedsbrud, drager konklusioner på baggrund af bruddet, og som gør erfaringerne tilgængelige for øvrige myndigheder og virksomheder.
- Der bør være en indberetningspligt ved tab af kontrol med følsomme og fortrolige personoplysninger.
- Lovgivningsinitiativer bør være teknologineutrale. Anvendelsen af personoplysninger samt konsekvenser for privatlivets fred – herunder hvordan negative konsekvenser for privatlivets fred kan undgås – bør fremgå af bemærkninger til fremsatte lovforslag.

3.2 Tilsynet med overholdelse af persondataloven

Tilsynet med overholdelse af persondataloven bør hvile på principperne nævnt ovenfor.

Styrkelse af tilsynsmyndigheder

Arbejdsgruppen kan konstatere, at persondataloven i alt for mange tilfælde ikke overholdes af såvel offentlige myndigheder som private virksomheder.

Datatilsynet er tilsynsmyndighed for overholdelsen af lov om behandling af personoplysninger (persondataloven), og arbejdsgruppen vurderer, at der er et synligt behov for, at Datatilsynet fører et mere effektivt tilsyn med overholdelsen af persondataloven.

Arbejdsgruppen vil derfor opfordre til, at Datatilsynet tilføres de nødvendige ressourcer og beføjelser, så Datatilsynet og det effektive tilsyn med overholdelse af persondataloven styrkes.

Det er arbejdsgruppens overbevisning, at et mere ressourcestærkt tilsyn vil kunne øge informationsindsatsen, foretage flere inspektioner, tage flere sager op af egen drift, nedbringe sagsbehandlingstider og vejlede virksomheder og myndigheder om persondataloven for dermed at skærpe overholdelsen af de allerede eksisterende regler på persondataområdet.

Arbejdsgruppen anbefaler, at man bør overveje, hvorvidt Datatilsynets kontrolbesøg skal være risikobaserede. Det vil sige, at hyppigheden af Datatilsynets kontrolbesøg afgøres af, hvor kritiske, følsomme og fortrolige personoplysninger der behandles hos den offentlige myndighed eller private virksomhed.

Videre anbefaler arbejdsgruppen, at man ud over at styrke tilsynsmyndighederne også iværksætter en undersøgelse af, hvordan man kan styrke den tværfaglige videnopsamling og rådgivning af offentlige institutioner og private virksomheder.

Arbejdsgruppen noterer sig som tidligere nævnt, at regeringen vil invitere til en politisk drøftelse, hvor også en styrkelse af Datatilsynet skal drøftes, jf. REU alm. del – svar på spørgsmål 1240, folketingsåret 2013-14. Arbejdsgruppen ser frem til at drøfte, hvordan Datatilsynet og dermed tilsynet med overholdelse af persondataloven kan styrkes.

Arbejdsgruppen er opmærksom på, at også andre myndigheder fører tilsyn med myndigheder og virksomheder, som behandler følsomme og fortrolige personoplysninger. I den forbindelse noterer arbejdsgruppen sig, at effektiviteten af disse tilsyn også er afgørende for at sikre beskyttelsen af borgernes persondata.

Arbejdsgruppen noterer sig i den forbindelse, at der løbende og i forbindelse med Se og Hør-sagen har været en diskussion om indretningen af de tilsynsmyndigheder, der beskæftiger sig med myndigheder eller virksomheder, der behandler følsomme og fortrolige personoplysninger, jf. REU alm. del – svar på spørgsmål 1084 og svar på spørgsmål 1107, folketingsåret 2013-14.

Databeskyttelsesmyndighed under Folketinget

Rådet for Digital Sikkerhed har oplyst, at det støtter placering af en databeskyttelsesmyndighed under Folketinget, idet rådet ikke mener, at Datatilsynet med dets nuværende placering under Justitsministeriet lever op til den uafhængighed, der er fastsat i EU's charter for grundlæggende rettigheder, jf. REU alm. del – bilag 61, folketingsåret 2013-14.

Arbejdsgruppen noterer sig Rådet for Digital Sikkerheds anbefaling og opfordrer til, at regeringen nærmere undersøger, hvordan Datatilsynet kan tilknyttes Folketinget i stedet for Justitsministeriet, og hvilke fordele der vil være forbundet hermed. Arbejdsgruppen understreger vigtigheden af Datatilsynets fortsatte uafhængighed og understreger, at en eventuel tilknytning til Folketinget ikke vil medføre instruktionsbeføjelse over for Datatilsynet. Arbejdsgruppen henviser i den forbindelse til REU alm. del – svar på spørgsmål 97.

Arbejdsgruppen ser frem til at diskutere Datatilsynets tilknytning ved den førnævnte politiske drøftelse med regeringen om datasikkerhed, jf. REU alm. del – svar på spørgsmål 1240, folketingsåret 2013-14.

Klagenævn til vurdering af Datatilsynets afgørelser

Det fremgår ikke direkte af det nuværende databeskyttelsesdirektiv, om der kan etableres en klageinstans til at behandle klager over Datatilsynets afgørelser. Det er imidlertid Justitsministeriet umiddelbare vurdering, at direktivet ikke er til hinder for en sådan ordning, jf. REU alm. del – svar på spørgsmål 1604, folketingsåret 2013-14.

Arbejdsgruppen mener, at dette bør overvejes for at sikre retssikkerheden, særlig i forbindelse med de udvidede sanktioner, der nævnes i det nuværende forordningsforslag.

Anmeldelsesordning

Som udgangspunkt skal enhver behandling af fortrolige oplysninger anmeldes til Datatilsynet. Arbejdsgruppen note-

rer sig i den forbindelse, at 2.777 ud af Datatilsynets 6.118 sager i 2013 vedrørte anmeldelser, jf. REU alm. del – bilag 400, folketingsåret 2013-14.

I den forbindelse bemærker arbejdsgruppen, at anmeldelsesordningen indeholdt i den nuværende persondatalov og i det gældende databeskyttelsesdirektiv ikke videreføres i det nuværende forslag til en kommende databeskyttelsesforordning, der i øjeblikket forhandles i EU, jf. REU alm. del – svar på spørgsmål 1603, folketingsåret 2013-14. I stedet lægges der i forslaget op til, at den dataansvarlige skal opbevare optegnelser over behandlinger af personoplysninger, og at databehandler skal opbevare optegnelser over behandlinger af personoplysninger, når behandlingerne foretages på den dataansvarliges vegne.

Arbejdsgruppen noterer sig, at en ændring i den nuværende anmeldelsesordning med udgangspunkt i forordningsforslaget vil frigøre ressourcer hos Datatilsynet, som i stedet vil kunne bruges til at styrke tilsynet og øge antallet af kontrolbesøg. Arbejdsgruppen anbefaler derfor regeringen at undersøge dette.

3.3 Øgede sanktionsmuligheder ved brud på datasikkerhed

Datatilsynet har på nuværende tidspunkt ikke bemyndigelse til at udstede bøder, og i tilfælde af tvangsbøder er det domstolene, der udsteder disse. Justitsministeren oplyser, at det ifølge det nuværende persondatadirektiv er op til den enkelte medlemsstat af fastsatte regler om, hvilke sanktioner der skal være forbundet med overtrædelser af nationale bestemmelser om behandling af personoplysninger, jf. REU alm. del – svar på spørgsmål 1605, folketingsåret 2013-14.

Forordningsforslaget lægger i sin nuværende form op til, at tilsynsmyndighederne tildeles beføjelse til at udstede administrative bøder. Arbejdsgruppen noterer sig, at justitsministeren bemærker, at det ifølge grundlovens § 3 må antages, at lovgivningsmagten ikke kan henlægge behandling af strafferetlige bødesager til administrative myndigheder, jf. REU alm. del – svar på spørgsmål 1605, folketingsåret 2013-14.

Arbejdsgruppen noterer sig, jf. ovenstående princip om et stærkt tilsyn, at et effektivt tilsyn bør have tilstrækkelige sanktionsmuligheder. Arbejdsgruppen er enig om, at Datatilsynets nuværende sanktionsmuligheder ikke er tilstrækkelige, og at der er behov for, at yderlige 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. Der henvises til REU alm. del – svar på spørgsmål 178.

Sanktionsmuligheder i forhold til offentlige myndigheder

Ifølge persondataloven kan Datatilsynet foretage inspektioner for at undersøge, om personoplysninger behandles lovligt. Arbejdsgruppen noterer sig imidlertid, at der er forskel på Datatilsynets sanktionsmuligheder, afhængigt af om bruddet på persondataloven vedrører en offentlig myndighed eller en privat virksomhed. Datatilsynet kan udelukkende udstede forbud og påbud til private, hvilket imidlertid ikke er muligt i forhold til offentlige myndigheder, jf. § 59 i lov om behandling af personoplysninger. Over for private kan der yderligere tildeles tvangsbøder for at opnå overholdelse af Datatilsynets afgørelser, hvilket heller ikke er muligt over for offentlige myndigheder.

Arbejdsgruppen mener, at offentlige myndigheder og private virksomheder bør gøres til genstand for samme sanktionsmuligheder, og noterer sig, at denne ligestilling efter arbejdsgruppens opfattelse også er udgangspunktet i det foreliggende forslag til forordning.

Sanktionsmuligheder i forhold til databehandler

Arbejdsgruppen noterer sig, at den dataansvarlige som udgangspunkt er pligtsubjekt i persondataretten, og at denne er ansvarlig for, at persondataloven overholdes. Justitsministeren oplyser i sit svar på REU alm. del – svar på spørgsmål 92, at den dataansvarlige, jf. persondatalovens § 4, stk. 3, 1. pkt., skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltning for at sikre, at oplysninger ikke tilintetgøres, fortabes, forringes eller kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Arbejdsgruppen bemærker dog, at det af justitsministerens svar fremgår, at »Bestemmelsen [§ 41, stk. 3, 2. pkt.] antages at skulle forstås sådan, at der er tale om en selvstændig pligt for databehandleren til at sørge for, at kravene i § 41, stk. 3, 1. pkt., bliver overholdt i forbindelse med behandlingen ...«, jf. REU alm. del – svar på spørgsmål 91. Derfor anbefaler arbejdsgruppen, at det udredes, hvad databehandlers ansvar er i forhold til at sikre personoplysninger og overholde persondataloven, og hvordan databehandleres ansvar defineres i forhold til dataansvarliges ansvar.

Arbejdsgruppen finder, at det er afgørende for sikkerheden omkring personoplysninger, at databehandler gøres juridisk ansvarlig for overholdelse af persondataloven. Derfor opfordres regeringen på baggrund af førnævnte udredning til at igangsætte de fornødne initiativer, herunder eventuelle lovgivningsinitiativer, så databehandler også gøres til pligtsubjekt i persondataretten.

3.4 Samling af ansvaret for datasikkerhed

I beretning nr. 3 af 3. juni 2014 om nedsættelse af en parlamentarisk arbejdsgruppe gjorde Kulturudvalget og Retsudvalget opmærksom på behovet for samling af datasikkerhed ved en ansvarlig ressortminister. Arbejdsgruppen noterer sig, at Statsrevisorerne i deres bemærkning til Rigsrevisionens »Beretning om statens behandling af fortrolige oplysninger om personer og virksomheder« (nr. 1/2014) af november 2014 nævner, at en uklar ansvarsplacering mellem flere myndigheder kan svække tilsyn og datasikkerhed (REU alm. del – bilag 62).

Arbejdsgruppen har i lighed med Rigsrevisionen noteret sig, at ansvarsfordelingen mellem flere ministerier på datasikkerhedsområdet kan være en udfordring for en effektiv databeskyttelse.

Arbejdsgruppen opfordrer statsministeren til at overveje det hensigtsmæssige i, at datasikkerhedsområdet fremover samles hos én ansvarlig minister. I den forbindelse skal det understreges, at arbejdsgruppen anerkender, at det er op til den siddende statsminister at foretage ændringer i ministeriernes ressortområder.

Arbejdsgruppen opfordrer desuden til, at datasikkerhedsområdet samles under et dertil særligt indrettet udvalg under Folketinget fra næste folketingsår. Arbejdsgruppen vil kontakte Folketingets Præsidium herom.

3.5 Tekniske krav til sikring af følsomme og fortrolige personoplysninger

Det er arbejdsgruppens overbevisning, at en række tekniske tiltag kan øge datasikkerheden hos offentlige myndigheder og virksomheder.

Implementering af privacy by design

Arbejdsgruppen mener, at hensynet til borgernes privatliv skal være et naturligt udgangspunkt, når it-systemer designes og udvikles.

Arbejdsgruppen anbefaler derfor regeringen at inddrage princippet om privacy by design i fremtidige offentlige it-systemer. Desuden opfordres regeringen til at tage de fornødne initiativer, så princippet om privacy by design bliver indført som et krav til samtlige leverandører af offentlige it- og digitaliseringsløsninger.

Videre anbefaler arbejdsgruppen, at de nuværende offentlige it-systemer opgraderes, så de lever op til principperne for privacy by design.

Sikkerhedsstandarden ISO 27001

De statslige institutioner er fra januar 2014 blevet pålagt at følge den internationale sikkerhedsstandard ISO 27001. Samtidig har arbejdsgruppen noteret sig, at en lang række organisationer, der arbejder med datasikkerhed, anser ISO 27001 som værende et egnet redskab til at øge sikkerheden omkring følsomme og fortrolige personoplysninger.

Arbejdsgruppen støtter, at implementeringen af ISO 27001 i statslige institutioner fremskyndes.

Kontrol af rollebaseret adgang

Af sikkerhedsbekendtgørelsens § 11, stk. 2, og § 17, stk. 1 og 2, fremgår det, at brugernes adgang til personoplysninger skal være betinget af, om brugerne har behov for oplysningerne til at løse deres arbejdsopgaver.

Arbejdsgruppen bemærker, at den seneste beretning fra Rigsrevisionen viser, at kontrol med brugernes adgang til personoplysninger ikke er tilfredsstillende i størstedelen af de undersøgte statslige institutioner.

Arbejdsgruppen mener derfor, at der bør følges op på kontrollen med brugeradgang til personoplysninger i de statslige institutioner. Arbejdsgruppen anbefaler ligeledes, at opfølgning på kontrol med brugeradgange indskrives som krav i offentlige udbudskontrakter.

3.6 Øvrige bemærkninger

Under henvisning til ovenstående princip om samtykke til salg og udnyttelse af følsomme og fortrolige personoplysninger anbefaler arbejdsgruppen, 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.

Arbejdsgruppen mener, at der bør foretages en kortlægning af eksisterende offentlige registre, jf. ovenstående princip om registrering. I forbindelse med kortlægningen bør det overvejes, om der i nogle tilfælde registreres og opbevares mere data end nødvendigt.

Arbejdsgruppen anbefaler, at der udarbejdes en national strategi for informations- og datasikkerhed for den samlede offentlige sektor. I den forbindelse noterer arbejdsgruppen sig, at regeringens »National strategi for cyber- og informationssikkerhed« (december 2014) sætter fokus på cyber- og informationssikkerhed i de statslige myndigheder samt i tele- og energisektoren.

Arbejdsgruppen mener, at brugen af cpr-nummeret bør gennemgå en grundlæggende revidering. Herunder mener arbejdsgruppen, at opgivelse af cpr-nummer ikke alene skal kunne udgøre autentificering, samt at man i forberedelsen af næste generation af digital id bør medtænke, at cpr-nummeret eventuelt afvikles som gennemgående id i offentlige registre. Arbejdsgruppen noterer sig i den forbindelse, at daværende økonomi- og indenrigsminister Margrethe Vestager orienterede Folketingets Kommunaludvalg om, at ministeren grundigt ville overveje, hvilke konsekvenser sagen om lækket af 900.000 cpr-numre skulle have, og at ministeren ville orientere udvalget om resultatet af disse overvejelser, jf. KOU alm. del – svar på spm. 108, folketingsåret 2013-14. Arbejdsgruppen ser frem til denne orientering.

P.u.v.

Karina Lorentzen Dehnhardt

formand

Bilag 1

Oversigt over bilag af relevans for beretningen

Bilagsnr. 2014/15	Titel
9	Program til åben høring den 22. oktober 2014 om offentlige myndigheders behandling af personoplysninger
12	Brev til justitsministeren ang. besvarelse af REU alm. del – spørgsmål 1240
14	Henvendelse af 18/10-14 fra Kai V. H. Jensen om Folketingets Datahøring den 22. oktober 2014
17	Notat af Kim Normann Andersen fra CBS vedr. Sikkerhedsproblemer i håndtering af persondata i.f.m. det offentliges digitale kommunikation med borgerne
20	Henvendelse af 20/10-14 fra DI ITEK vedr. metode til beskyttelse af privatlivets fred
21	Præsentationer fra høringen den 22. oktober 2014 om offentlige myndigheders behandling af personoplysninger
22	Janne Glæsels præsentation fra arbejdsgruppemødet i arbejdsgruppen om datasikkerhed den 23. oktober 2014
26	Brev til applikationsudbydere, fra arbejdsgruppen om datasikkerhed
32	Udkast til program til høring om tekniske krav til sikring af følsomme personoplysninger den 12. november 2014
54	Offentligt høringsprogram den 12. november 2014
60	Materiale fra høring den 12. november 2014 om tekniske tiltag til sikring af følsomme personoplysninger
61	Henvendelse af 13/11-14 fra Rådet for Digital Sikkerhed om regeringens plan for digital vækst
62	Statsrevisorernes beretning 1/2014 om statens behandling af fortrolige oplysninger om personer og virksomheder
77	Parlamenterne i Tysklands, Storbritanniens, Norges og Sveriges svar på, hvordan personoplysninger behandles i de pågældende lande
78	Fællesbrev til arbejdsgruppen vedr. beskyttelse af personfølsomme oplysninger (under Kulturudvalget og Retsudvalget) med en fælles opfordring til revision af de danske logningsregler fra en bred kreds af relevante aktører
127	Internt dokument: Kommentarer til beretning om datasikkerhed
128	Notater fra parlamenterne i Tyskland, Storbritannien, Norge og Sverige, om hvordan personoplysninger behandles i de pågældende lande
130	Internt dokument: Svar på arbejdsgruppen om datasikkerheds henvendelse i oktober 2014 til en række danske og udenlandske applikationsudbydere, som via mobile apps får adgang til personlige oplysninger
135	Internt dokument: Udkast til beretning om datasikkerhed
136	Henvendelse af 14/1-15 fra Finansrådet om apps adgang til at indhente informationer fra brugerne
144	Offentlige svar på arbejdsgruppen om datasikkerhed under Retsudvalgets henvendelse i oktober 2014 til en række danske og udenlandske applikationsudbydere, som via mobile applikationer får adgang til personlige oplysninger.

2013-14

289 Kulturudvalgets og Retsudvalgets beretning nr. 3 af 3. juni 2014 om nedsættelse af en parlamentarisk arbejdsgruppe, der skal undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med offentlige institutioner såvel som private virksomheders behandling af disse

353 Rapport fra august 2014 vedrørende hackerangrebet mod CSC, Center for Cybersikkerheds, og Digitaliseringsstyrelsens

358 Materiale fra dialogmødet den 26. august 2014 i arbejdsgruppen om datasikkerhed under Retsudvalget

364 Høringssvar til beretning om nedsættelse af en parlamentarisk arbejdsgruppe

367 Brev til Justitsministeriet m.fl. vedr. nedsættelse af den parlamentariske arbejdsgruppe, som skal undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger.

369 Høringsnotat – arbejdsgruppen om datasikkerhed under Retsudvalget

376 Internt dokument: Lotte Rickers Olesens oplæg om forslag til en ny europæisk databeskyttelse

400 Materiale til møde den 30. september 2014 i arbejdsgruppen om datasikkerhed

Oversigt over spørgsmål og svar af relevans for beretningen

Spm.nr.	**Titel**
2014-15	**REU alm. del**
90	Spørgsmål om, hvilke krav og regler angående datasikkerhed der er gældende for private virksomheder, der beskæftiger sig med kritisk infrastruktur, til justitsministeren, og ministerens svar herpå
91	Spørgsmål om særlig kontrol med private virksomheder, der beskæftiger sig med kritisk infrastruktur, til justitsministeren
92	Spørgsmål om, hvor i persondataloven det er fastsat, at det som udgangspunkt er den dataansvarlige, der er ansvarlig for overholdelse af persondataloven, til justitsministeren, og ministerens svar herpå
97	Spørgsmål om, hvor mange gange Datatilsynet siden sin oprettelse for 14 år siden har gennemført inspektioner/kontrolbesøg hos Justitsministeriets departement med henblik på at påse departementets overholdelse af persondataloven, til justitsministeren, og ministerens svar herpå
178	Spørgsmål om, hvilke straffebestemmelser der er gældende, når personer uberettiget skaffer sig adgang til og misbruger andres it-systemer ved enten at gøre sig bekendt med oplysningerne eller ved at slette, ændre, kopiere, videregive eller videresælge data, til justitsministeren, og ministerens svar herpå
180	Spørgsmål om, hvilken betydning Wassenaaraftalen har for forskning i kryptering og udvikling af kryptering, herunder krypteringssystemer- og produkter, til erhvervs- og vækstministeren, og ministerens svar herpå

2013-14

1084 Spørgsmål om, hvorfor Finanstilsynet ikke har været på besøg hos Nets og undersøge godkendelserne af PCI-standarderne, til erhvervs- og vækstministeren, og ministerens svar herpå

1107 Spørgsmål, om ministeren på baggrund af den konkrete sag fra Nets om misbrug af fortrolige kreditkortoplysninger har anmodet Finanstilsynet om en nærmere redegørelse om Finanstilsynets tilsynsvirksomhed og it-sikkerhedsinspektioner i Nets, til erhvervs- og vækstministeren, og ministerens svar herpå

1240 Spørgsmål om at undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med offentlige institutioner såvel som private virksomheders behandling af disse, til justitsministeren, og ministerens svar herpå

1603 Spørgsmål, om de gældende EU-regler og de EU-regler, der aktuelt er under gennemførelse, kan erstatte de eksisterende anmeldelsesordninger for virksomheder og myndigheder med udpegningen af en data protection officer, til justitsministeren, og ministerens svar herpå

1604 Spørgsmål om en ordning, hvor der ud over et datatilsyn er etableret et selvstændigt klagenævn, til justitsministeren, og ministerens svar herpå

1605 Spørgsmål, om Danmark vil kunne give Datatilsynet hjemmel til at udstede bøder til henholdsvis private virksomheder og offentlige myndigheder for overtrædelse af datasikkerhedsbestemmelserne, til justitsministeren, og ministerens svar herpå