

ARBEJDSGRUPPEN OM DATASIKKERHED UNDER RETSUDVALGET

FOLKETINGET



NOTAT

Høringsnotat om beretning nr. 3 afgivet af Folketingets Kulturudvalg og Retsudvalg

8. september 2014

Folketinget sendte den 2. juli 2014 beretning 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 i høring med frist den 29. august 2014.

Birgitte Toft-Petersen
Udvalgssekretariatet
Birgitte.Toft-Petersen@ft.dk

Der er i overensstemmelse med beretningen blevet nedsat to arbejdsgrupper under henholdsvis Kulturudvalget og Retsudvalget. Begge arbejdsgrupper har sendt beretningen i høring hos udvalgte interessenter (se vedlagte høringsliste for arbejdsgruppen under Retsudvalget, bilag 2).

Til arbejdsgruppen under Retsudvalget har i alt 30 organisationer m.v. afgivet høringssvar inden for høringsfristen (bilag 1). Blandt disse har Dansk Kredit Råd, Den Danske Dommerforening, Domstolsstyrelsen, Konkurrence- og Forbrugerstyrelsen, Københavns Byret, LO, Rigsrevisionen, Vestre Landsret, og Østre Landsret tilkendegivet, at de ikke har nogen bemærkninger.

I det følgende redegøres tematisk for hovedsynspunkterne i de modtagne høringssvar til beretning nr. 3. Der henvises herudover til de samlede høringssvar (bilag 3).

1. Resumé

CSC Danmark A/S, Dansk Industri, Finansrådet, Forbrugerrådet Tænk, Institut for Menneskerettigheder, lektor Trine Baumbach, Ingeniørforeningen IDA, IT-Branchen og professor Jørn Vestergaard anfører, at det er positivt, at Folketingets Retsudvalg sætter fokus på datasikkerhed og databeskyttelse.

Dansk Industri, DANSK IT, Dansk Journalistforbund, Datatilsynet, Finansrådet, Forbrugerombudsmanden, Ingeniørforeningen IDA, IT-Branchen, IT-Politisk Forening, KL og Sikkerhedsbranchen anfører, at de gerne stiller sig til rådighed for arbejdet i arbejdsgruppen.

1.1. Arbejdsgruppens struktur

KL anbefaler, at kredsen af eksperter, der er tiltænkt at indgå i arbejdet, udvides, og finder det hensigtsmæssigt, at KL inddrages.

Danske Regioner anbefaler, at der inddrages repræsentanter fra de

interessenter, der bruger data. De mener derfor, at Danske Regioner, KL, Datatilsynet og repræsentanter fra forskningsområdet bør inddrages i arbejdsgruppens arbejde.

IT-Politisk Forening mener ikke, at arbejdsgruppens tidshorisont er realistisk, hvis arbejdsgruppen skal producere en substantiel analyse af de danske databeskyttelsesproblemer.

KL og Danske Regioner mener, at der bør lægges vægt på de økonomiske og forvaltningsmæssige konsekvenser ved implementering af arbejdsgruppens anbefalinger og pålægning af nye opgaver.

IT-Branchen mener, at der aktivt bør inddrages eksperter fra virksomheder, der har praktisk erfaring på området.

1.2. Registrering af data

Ingeniørforeningen IDA mener, at der er mange fordele ved at styrke digitaliseringen af Danmark, men hvis fordelene skal høstes, er det afgørende, at danskerne ikke lægger bånd på sig selv i deres brug af internettet.

Ingeniørforeningen IDA mener dog, at borgerne ofte slet ikke er klar over, hvad der registreres, og mener, at kommunikation med det offentlige skal krypteres efter principperne om anbefalet post. Foreningen understreger, at antallet af centrale databaser er stigende, hvilket øger muligheden for at sammenkæde oplysninger om borgerne.

IT-Politisk Forening påpeger, at det er vigtigt at overveje antallet af centrale databaser, når initiativer som for eksempel rejsekortet, fjernaflæste elmålere og roadpricing diskuteres.

CPR-registeret

IT-Politisk Forening anfører, at mange offentlige ansatte har adgang til følsomme personoplysninger via CPR-registeret, hvilket skaber en større risiko for misbrug, ligesom systemfejl, datalæk eller hackerindbrud også er en risiko ved registret.

Forbrugerombudsmanden mener, at det er et stigende problem, at forbrugernes cpr-nummer ofte afkræves i forbindelse med aftaleindgåelse uden saglig begrundelse.

Ingeniørforeningen IDA mener, at det danske CPR-register og den elektroniske patientjournal (EPJ) er et positivt eksempel på anvendelse af Big data i forbindelse med eksempelvis kræftforskning og sundhedsanalyser.

Big data

Ingeniørforeningen IDA fremhæver, at et afgørende karaktertræk ved Big data er, at virksomheder ikke kun anvender egne data men også data fra kunder, leverandører, offentlige registre, sociale medier m.v. Ved hjælp af nye

typer algoritmer og bedre computere kan databehandlingen være med til at styrke virksomheders beslutningsgrundlag. Ingeniørforeningen IDA mener derfor, at Big data vil være en af de store fremtidige kilder til produktudvikling, men det stiller samtidig øgede krav til sikkerhed og etik omkring brugen af data.

Ingeniørforeningen IDA anbefaler også, at stat, regioner og kommuner stiller ikkepersonfølsomme data til rådighed og fri afbenyttelse, og at der oprettes en portal for private virksomheders køb og salg af ikkepersonfølsomme data.

Danske Medier anerkender værdien af kommerciel udnyttelse af Big data, mens de bifalder, at arbejdsgruppen vil se på anonymisering, så Big data fortsat kan benyttes optimalt.

Danske Regioner anfører, at brug af data er en forudsætning for kommunale og regionale kerneopgaver og for at skabe innovation og vækst bl.a. i forhold til bedre behandlingsformer i sundhedsvæsenet.

Forbrugerombudsmanden fremhæver, at indsamling af oplysninger om forbrugeradfærd kan bruges til målrettet markedsføring og behavioral pricing og mener, at der bør iværksættes en EU-undersøgelse til at belyse problemstillingen.

Forbrugerrådet Tænk mener, at der er behov for klare regler for indsamling, anvendelse og videresalg af Big data, idet brugen af Big data ikke klart er reguleret i persondataloven. Det anbefales derfor, at der fastsættes regler på området, som kan skabe gennemsigtighed, og som kan sikre en balance mellem den kommercielle interesse for data og forbrugernes ret til privatliv.

1.3. Tilsyn

Institut for Menneskerettigheder mener generelt, at den tværfaglige rådgivning og tilsynet med databeskyttelse og informationssikkerhed bør styrkes, og Dansk Journalistforbund mener, at der skal være et bedre tilsyn med efterlevelsen af de eksisterende krav til databeskyttelse.

Rigsrevisionen har i udgangspunktet ikke kommentarer til beretningen, men vil gerne gøre opmærksom på, at Rigsrevisionen kan undersøge, om virksomheder efterlever persondatalovens bestemmelser. I den forbindelse forventer Rigsrevisionen at afgive beretning om statslige virksomheders beskyttelse af personoplysninger og virksomhedsdata til Statsrevisorerne i efteråret 2014.

IT-Branchen er af den opfattelse, at de eksisterende regler på området er tilstrækkelige, men at der kan være behov for at præcisere visse bestemmelser med henblik på at sikre korrekt efterlevelse af reglerne i virksomheder og organisationer.

Datatilsynet

DANSK IT, DI, Ingeniørforeningen IDA og Sikkerhedsbranchen støtter en styrkelse af Datatilsynet.

DANSK IT støtter, at Datatilsynet bliver styrket, så behandling af sager ikke er forsinkende for virksomheder.

DI mener, at Datatilsynet har behov for at blive styrket i takt med det stigende omfang af sager, som digitaliseringen har betydet. DI synes især, at styrkelsen af Datatilsynet bør ske på den tekniske front, så nye teknologier til brug ved behandling af personoplysninger og datasikkerhedsteknologier kan vurderes.

Ingeniørforeningen IDA støtter en styrkelse af Datatilsynet, så tilsynet også kan rådgive om Big data, udstikke retningslinjer på niveau med ombudsmanden og gøres uafhængig. Ingeniørforeningen IDA tilføjer, at Datatilsynet kunne suppleres med datarevisorer, som det kendes fra regnskabsrevisorer.

Det er **Sikkerhedsbranchens** opfattelse, at tilsynet allerede under den eksisterende lovgivning har behov for en øget bevilling.

KL mener, at kendskabet til de allerede gældende regler for databeskyttelse kan udbredes bl.a. ved at styrke og udvide Datatilsynets opgaver.

CSC Danmark A/S mener derimod ikke, at en styrkelse af Datatilsynet i sig selv vil gøre offentlige systemer mere sikre. Det vil i stedet have anvisninger og anbefalinger, der instruerer offentlige myndigheder i, hvordan it-systemer skal sikres og overvåges. En styrkelse af offentlig tilsynsvirksomhed bør derfor ifølge CSC Danmark A/S have stærke it-sikkerhedsmæssige kompetencer.

Forbrugerrådet Tænk mener, at Datatilsynets tilgang til databeskyttelse i dag er stringent juridisk, og efterlyser et tilsyn, der lægger vægt på at integrere persondataregler med private og offentlige virksomheders brug af privatlivsfremmende it-løsninger. Forbrugerrådet Tænk mener derfor, at en ekstrabevilling til et stærkere tilsyn bør betinges af et større fokus på integration af jura og teknologi, uafhængighed samt rådgivning til offentlige og private virksomheder.

Forbrugerrådet Tænk mener også, at tilsynet kan styrkes ved at indføre en pligt for virksomheder til at anmelde databrud og øge det nuværende bødeniveau. **Ingeniørforeningen IDA** mener også, at firmaer bør have pligt til at oplyse, når der sker datalæk, og at firmaerne bør bære de økonomiske omkostninger ved »oprydning« efter datalæk.

Datatilsynet mener, at overvejelser om at styrke Datatilsynet ikke alene bør fokusere på omfanget af ressourcer, men også på indholdet af de opgaver, som Datatilsynet forventes at varetage. Det kan f.eks. overvejes, om tilsynet fortsat i samme udstrækning som i dag skal udstede tilladelser til virksomheder og behandle anmeldelser fra offentlige myndigheder, der behandler fortrolige oplysninger som naturlig følge af deres myndighedsudøvelse. Datatilsynet understreger, at tilsynet udøver sine funktioner i fuld uafhængighed.

I forbindelse med Datatilsynet anfører **lektor Trine Baumbach**, at medier omfattet af medieansvarsloven i vidt omfang ikke er omfattet af persondataloven og dermed ikke omfattet af Datatilsynets kontrol eller

tilsvarende kontrol. Det synes derfor nødvendigt at granske, hvorvidt der er behov for en bedre beskyttelse af de personfølsomme oplysninger, som pressen kommer i besiddelse af.

DI mener, at det ville være nyttigt, hvis der afleveres en årlig redegørelse i form af en kortlægning af sikkerhedsniveauet i den offentlige sektor til Folketinget, hvilket også **Danske Regioner** synes er en konstruktiv idé.

1.4. It-modeller og sikkerhedsløsninger

Institut for Menneskerettigheder mener, at der behov for en bredere undersøgelse af, hvordan man kan forbedre sikkerheden ved behandling af personoplysninger i den offentlige sektor, herunder en kritisk gennemgang af gældende regelsæt, en analyse af interne og eksterne kontrolmekanismer og et eventuelt behov for at styrke disse.

IT-Branchen gør opmærksom på, at de arbejder på at udvikle »en fælles ramme«, der kan bruges af leverandører, myndigheder og virksomheder til at skabe et overblik over, hvilket sikkerhedsniveau der ønskes, samt hvilke krav, sikkerhedspolitikker og kontroller man derfor bør efterleve. IT-Branchen orienterer om, at man gerne møder arbejdsgruppen om denne fælles ramme ved for eksempel et foretræde.

Udpegning af dataansvarlig

Forbrugerrådet Tænk mener, it-sikkerhed og databeskyttelse skal være et centralt anliggende og ansvar for direktionen i både offentlige og private virksomheder og ikke kun it-chefens alene.

Hi3G Denmark ApS (herefter: **3**) oplyser, at de har dedikeret en information security manager til løbende at sikre og overvåge, at data håndteres i overensstemmelse med gældende lovgivning.

KL mener, at ideen om at have en databeskyttelsesansvarlig ansat til særskilt at holde fokus på datasikkerheden i den enkelte myndighed er en god idé, men de mener ikke, at det skal være et krav, idet det vil forhindre kommunerne i at tilpasse arbejdet med datasikkerhed til den enkelte kommune.

Udbredelse af ISO 27001

DANSK IT anbefaler, at arbejdsgruppen undersøger, hvorvidt private virksomheder og hele den offentlige sektor bør anvende fælles informationssikkerhedsstandarder, og om det offentliges sikkerhedsstandard ISO 27001 kan bredes ud til andre dele af samfundet.

Forbrugerrådet Tænk mener også, at udbredelsen af ISO 27001 skal sikres af regeringen.

Institut for Menneskerettigheder mener, at der er behov for en styrket kontrol med offentlige it-projekter og leverandørers efterlevelse af de

standarder for informationssikkerhed og databeskyttelse, der er foreskrevet i sikkerhedsbekendtgørelsen og ISO 27001.

DI mener også, at der skal føres et mere systematisk tilsyn med, om den offentlige sektor og dens leverandører efterlever ISO 27001, end hvad tilfældet er ved Rigsrevisionens tilsyn i dag.

Privacy impact assessments (privatlivskonsekvensanalyser)

DI mener, at der ved behandling af personoplysninger bør udarbejdes en skabelon for privacy impact assessments (herefter: PIA). **DI** mener, at skabelonen bør gøres obligatorisk ved alle større, offentlige it-projekter. Udgangspunktet for skabelonen bør være, om det overhovedet er nødvendigt at identificere borgeren, og i givet fald hvornår i processen identifikation af borgeren er nødvendig. **DI** mener, at dette i nogle sammenhænge vil give en bedre beskyttelse af personoplysninger, end det kan opnås ved den PIA-skabelon, som Digitaliseringsstyrelsen har udarbejdet.

Forbrugerrådet Tænk mener også, PIA-analyser bør gøres obligatoriske for offentlige og private virksomheder. Forbrugerrådet Tænk mener, at man med fordel kan tage udgangspunkt Digitaliseringsstyrelsens PIA-håndbogen.

Institut for Menneskerettigheder mener, at PIA skal indarbejdes som fast obligatorisk praksis ved offentlige it-projekter. I den forbindelse mener Institut for Menneskerettigheder, at den canadiske model og praksis kan tjene som inspiration.

Ingeniørforeningen IDA mener, at der bør være en obligatorisk vurdering af databeskyttelse for både offentlige og private digitaliseringsprojekter, når der behandles offentlige data.

Danske Regioner mener, at det er fornuftigt at iværksætte en nærmere undersøgelse af, hvorvidt der skal være en obligatorisk databeskyttelsesvurdering i digitale projekter, og at det bør overvejes, om det også skal være tilfældet for den private sektor.

Privacy by design

DI mener, at der bør opstilles en række helt overordnede designprincipper, så god sikkerhed indledningsvis designes ind i it-løsninger. I it-løsningerne bør der også indarbejdes privatlivsfremmende teknologier som anonymisering, pseudonomisering, rollebaseret adgangskontrol og logning.

Forbrugerrådet Tænk mener også, at der er behov for et øget brug af privatlivsfremmende teknologier, og mener, at man kan erstatte den nuværende brede adgang med en rollebaseret adgang.

Forbrugerrådet Tænk anbefaler, at regeringen indhenter erfaring med dansk og udenlandsk brug af privatlivsfremmende teknologier.

Ingeniørforeningen IDA understreger, at man bør støtte op om brugen af design af personfølsomme data efter principperne i privacy by design, så data

bliver brugbare i anonym form og data ikke ved hjælp af samkøring med andre data kan de-anonymiseres.

Ingeniørforeningen IDA mener, at en effektiv anonymisering af datasæt til brug ved forskning og kommercielle formål er et vigtigt indsatsområde, og mener, at der skal indføres krav til indførelse af privacy by design og privacy by default.

Institut for Menneskerettigheder mener, at privacy bør tænkes ind som en naturlig og obligatorisk komponent i forbindelse med design af nye offentlige it-systemer, og Danske Regioner mener, at det er positivt, at mulighederne for at anonymisere data undersøges og konkretiseres.

IT-Politisk Forening foreslår, at arbejdsgruppen orienterer sig i rapporten »Nye digitale sikkerhedsmodeller – et diskussionspapir« fra IT- og Telestyrelsen, når arbejdsgruppen skal undersøge privacy by design og indretningen af de offentlige systemer.

Ingeniørforeningen IDA mener desuden, at private og offentlige virksomheder bør oprette brugeradgang til de oplysninger, som den pågældende virksomhed har om brugeren, og som ikke bliver slettet, når brugeren forlader siden.

1.5. Forordning om databeskyttelse

DI, Forbrugerrådet Tænk og Ingeniørforeningen IDA støtter EU's persondataforordning.

DI mener, at der er vigtigt, at Danmark er imødekommende over for Europa-Kommissionens forslag til en persondataforordning. Det skyldes, at DI mener, at der er behov for harmonisering, og at forordningen stiller krav om udarbejdelse af privacy impact assessments og arbejdet med privacy by Design.

Forbrugerrådet Tænk mener, at et klart mandat fra Danmark er afgørende, hvis forordningen skal vedtages i Rådet. Forbrugerrådet mener, at der – inden forordningen vedtages – bør stilles lovmæssige krav i tråd med forordningen til både offentlige og privates brug af privatlivsfremmende teknologier.

Ingeniørforeningen IDA skriver, at en persondatalov, der tager højde for nye teknologier, bl.a. Big data og de sociale medier, er et vigtigt indsatsområde. Foreningen mener, at lovgivning er afgørende vigtigt som motivation til, at virksomhederne tager initiativ til databeskyttelse og investerer i kryptering.

Finansrådet mener, at eventuelle initiativer på baggrund af Se og Hør-sagen bør være i tråd med forordningen.

3 mener, at beslutninger om tiltag i forhold til persondata og tilsyn bør afvente resultatet af forhandlingerne om forordningen, herunder om det vil være muligt og hensigtsmæssigt at indføre danske særregler på området i tillæg.

KL og Danske Regioner er skeptiske over for EU's persondataforordning.

KL mener, at der er problemer med Europa-Kommissionens forslag til en forordning om databeskyttelse, og at der allerede i dag er tilstrækkelige regler for det offentlige behandling af data i kraft af eksempelvis forvaltningsloven, CPR-loven og sundhedsloven.

Ifølge KL består problemerne bl.a. i, at der ikke tages højde for forskellen på det private og det offentlige formål med databehandling, at tyngden af de nye regler ikke vil tilføre tilsvarende datasikkerhed til borgerne, at bødeniveauet er for højt, at der stilles krav til dyre og ifølge KL mindre anvendelige konsekvensanalyser, at forordningen vil besværliggøre og fordyre realiseringen af potentialerne i den fællesoffentlige digitaliseringsstrategi m.v.

Danske Regioner mener også, at den eksisterende lovgivning er tilstrækkelig til at sikre fortrolighed om personfølsomme oplysninger.

Danske Regioner mener endvidere, at der ikke er behov for at ændre på den nuværende danske linje i forhold til arbejdet med en ny EU-forordning om persondatabeskyttelse.

Retspolitisk Forening bemærker, at den nye dataforordning kun kan forventes i særdeles begrænset og kun indirekte omfang at tage stilling til indsamling, bearbejdning og videregivelse af data indsamlet af medlemslandenes efterretningstjenester eller retshåndhævende myndigheder. Retspolitisk Forening anbefaler derfor bl.a., at lovene om politiets og forsvarrets efterretningstjenester ændres, så videregivelse af private fortrolige oplysninger uden samtykke til udenlandske myndigheder eller private fysiske eller juridiske personer alene kan ske som led i et internationalt samarbejde om forebyggelse og bekæmpelse af forbrydelser, der er strafbare i Danmark. Oplysninger, der kan indebære en risiko for tortur, skal dog ikke kunne videregives.

I forbindelse med det europæiske samarbejde gør **Forbrugerombudsmanden** opmærksom på, at der i det europæiske håndhævelsessamarbejde på forbrugerområdet CPC mangler mulighed for at kunne gribe ind, hvis det medlemsland, hvorfra en grænseoverskridende overtrædelse udspringer fra, ikke foretager sig noget.

1.6. Viden og rådgivning om datasikkerhed

Forbrugerrådet Tænk mener, at der er behov for styrke forbrugeren gennem øget viden og kompetencer inden for it-sikkerhed og databeskyttelse og yde hjælp, så den enkelte forbruger i videst muligt omfang værner om egne data.

Forbrugerrådet Tænk opfordrer til, at der igennem en finanslovsbevilling sikres tilstrækkelig og uvildig information, rådgivning og støtte til forbrugere samt uddannelse af børn og unge.

Derudover mener Forbrugerrådet Tænk, at der er behov for rådgivning af både private og offentlige virksomheder om brugen af privatlivsfremmende teknologier.

DI mener, at der blandt alle parter i samfundet bør arbejdes på at forøge viden og opmærksomhed om informationssikkerhed og privatliv hos borgerne.

I den forbindelse mener DI, at Rådet for Digital Sikkerhed har bidraget væsentligt til debatten om datasikkerhed, og foreslår, at rådet får en mindre bevilling på Finansloven til at udføre sit arbejde, f.eks. 2 mio. kr. pr. år de næste 5 år.

KL anbefaler arbejdsgruppen at sætte fokus på, hvordan kendskabet til de allerede gældende regler for databeskyttelse udbredes bl.a. ved at styrke og udvide Datatilsynets opgaver.

Uddannelse

DI mener, at der bør tilvejebringes viden om informationssikkerhed i uddannelsessystemet, i takt med at borgerne møder forskellige it-systemer, og om, hvordan man arbejder med at skabe en sikkerhedskultur i organisationer.

KL mener, at mere uddannelse af de kommunale medarbejdere, der behandler persondata, vil styrke datasikkerheden i det offentlige.

Ingeniørforeningen IDA mener, at der er behov for en målrettet indsats i forhold til at styrke uddannelserne og efteruddannelserne i forhold til de kompetencer, der kræves ved håndtering af Big data.

Ingeniørforeningen IDA mener videre, at etik og moral-parametre skal fremmes på uddannelserne, så de unge kan sige fra, hvis kommende arbejdsgivere kræver uetiske ting af dem.

Ingeniørforeningen IDA mener, at man bør lave en indsats på uddannelsen af de it-specialister, der udvikler systemerne, og ved at lære folkeskolebørnene om at gebærde sig i det digitale samfund.

Ingeniørforeningen anbefaler, at der skabes de nødvendige forsknings- og uddannelsesmæssige miljøer i Danmark, så fremtidig kompetencer i forhold til Big data-analyseværktøjer sikres hos matematikere, dataloger, ingeniører m.v.

1.7. Internationale forhold

Forbrugerombudsmanden belyser, at adgangen til at kunne samarbejde med de amerikanske myndigheder om grænseoverskridende svindel på internettet bør forbedres, da en del af de virksomheder, der overtræder EU-reglerne, er etableret i USA. Forbrugerombudsmanden påpeger, at der i EU i nogen tid har været arbejdet på netop dette, og forbrugerombudsmanden mener derfor, at arbejdet i EU bør fortsættes, så man opnår konkrete tiltag.

Forbrugerombudsmanden mener, at der bør være mulighed for at lukke/blokere adgangen til hjemmesider, også hvor udbydere er etableret i lande uden for EU via fagedforbud, når der registreres åbenlyse overtrædelser af persondataloven og/eller markedsføringsloven.

Efterretningsarbejde

Forbrugerombudsmanden mener, at der bør være et mere effektivt internationalt samarbejde og bedre efterforskningsredskaber, herunder aftale om udveksling af fortrolige oplysninger mellem EU og USA bl.a. om, hvem der er ansvarlig for hjemmesider.

Retspolitisk Forening bemærker, at der er behov for en grundig bearbejdning af dataproblematikker, der kan henføres til grundlovens bestemmelser om brud på meddelelshemmeligheden. F.eks. finder Retspolitisk Forening det væsentligt at få præciseret, hvilket anvendelsesområde videregivelsesmuligheden af personoplysninger i FE-lovens § 3 har.

Retspolitisk Forening bemærker også, at idet Center for Cybersikkerhed er henlagt til Forsvarets Efterretningstjeneste, er der fri udveksling af oplysning mellem netsikkerhedstjeneste og den øvrige del af efterretningstjenester, og anbefaler, at det overvejes, om der er behov for den udvidede definition af en sikkerhedshændelse, og om der er behov for at undtage centerets virksomhed fra persondataloven.

Retspolitisk Forening anbefaler desuden, at Tilsynet med Efterretningstjenesterne får mulighed for at give efterretningstjenesterne og Center for Cybersikkerhed pålæg vedrørende behandling af personoplysninger.

1.8. Ensretning og centralisering

Institut for Menneskerettigheder anbefaler, at der udarbejdes en samlet strategi for informationssikkerhed og databeskyttelse i den offentlige sektor, hvor databeskyttelse og informationssikkerhed behandles i et tæt samspil mellem retlige standarder, organisation og teknologisk løsning.

CSC Danmark A/S påpeger, at der ikke er en koordineret og ensartet it-sikkerhed på tværs af ministerier, styrelser og andre offentlige myndigheder. Det skyldes, at der ikke eksisterer lovgivning eller forordninger, der anviser, hvordan forskellige typer af data skal beskyttes. De mener, at alle følsomme data og funktioner skal være indbefattet, uanset om de varetages af en offentlig eller privat virksomhed.

Ressortfordeling

Institut for Menneskerettigheder mener, at informationssikkerhed og databeskyttelse bør opprioriteres politisk, og at det bør forankres med både teknisk, organisatorisk og juridisk kompetence for eksempel i form af et ressortministerium, ombudsmand eller offentlig institution.

Danske Regioner understreger, at personfølsomme oplysninger ikke alene er reguleret af logningsregler og persondataloven, og at denne kompleksitet skal reflekteres i overvejelserne om, hvorvidt der er behov for en samling af it- og datasikkerhed ved én ansvarlig ressortminister.

CSC Danmark A/S mener, at der er behov for, at ansvaret for nationens it-sikkerhed samles ét sted. CSC Danmark A/S mener i øvrigt, at man ved

etablering af én central it-sikkerhedsmyndighed bør etablere et bredt samarbejde med alle it-leverandører for sikre en optimal informationsudveksling.

1.9. Yderligere bemærkninger

I forhold til Se og Hør-sagen mener **3**, at det er vigtigt at identificere, om det er mangler i de eksisterende lovgivningsmæssige krav til datasikkerhed, der har ført til sagen, eller om der alene er tale om en overtrædelse af allerede eksisterende lovgivning.

Finansrådet kan ikke genkende den såkaldte Se og Hør-sag som et symptom på den generelle sikkerhedstilstand i banksektoren, idet it-sikkerheden generelt vurderes til at være høj, samtidig med at der både personalemæssigt og økonomisk investeres i området.

Finansrådet oplyser desuden, at der i deres regi er nedsat en arbejdsgruppe vedrørende beskyttelse af fortrolige kundeoplysninger, hvor bankerne har indledt drøftelser om håndtering, regler, procedurer og mulige fremadrettede tiltag. Finansrådet vil i september afgive en rapport til Erhvervs- og Vækstministeriet med en tilbagemelding på, hvad sektoren vil foretage sig.

Sikkerhedsbranchen bemærker, at de støtter ideen om certificering og registrering af alle opsatte overvågningskameraer, og mener, at datasikkerheden herigennem vil kunne forbedres.

Politiforbundet gør opmærksom på, at der ikke bør gives bedre muligheder for beskyttelse af personfølsomme oplysninger, end der eksempelvis kan ydes for at beskytte forbundets medlemmer for offentliggørelse i henhold til offentlighedsloven.

IT-Branchen bemærker, at det er vigtigt, at eventuelle nye tiltag ikke unødigt vanskeliggør virksomheders og organisationers evne til at levere god og effektiv kundeservice.

2. Afslutning

Høringssvar behandles henholdsvis i arbejdsgruppen om medieetik og medieansvar under Kulturudvalget den 10. september 2014 og i arbejdsgruppen om datasikkerhed under Retsudvalget den 11. september 2014.

3. Bilag

Bilag 1. Organisationer med afgivet høringssvar

CSC Danmark A/S
Danmarks Medie- og Journalisthøjskole

Dansk Industri
DANSK IT
Dansk Journalistforbund
Dansk Kredit Råd
Danske Medier
Danske Regioner
Datatilsynet
Den Danske Dommerforening
Domstolsstyrelsen
Forbrugerombudsmanden
Forbrugerrådet Tænk
Finansrådet
Hi3G Denmark ApS
Ingeniørforeningen IDA
Institut for Menneskerettigheder
IT-Branchen
IT-Politisk Forening
Jørn Vestergaard, professor ved Københavns Universitet
Kommunernes Landsforening (KL)
Konkurrence- og Forbrugerstyrelsen
Københavns Byret
Landsorganisationen i Danmark (LO)
Politiforbundet
Retspolitisk Forening
Rigsrevisionen
Sikkerhedsbranchen
Trine Baumbach, lektor ved Københavns Universitet
Vestre Landsret
Østre Landsret

Bilag 2. Høringsliste

Accenture
Advokatrådet
Akademikernes Centralorganisation
Amnesty International
Arbejderbevægelsens Erhvervsråd
Borgerservice Danmark
Brancheforeningen Telekommunikationsindustrien
Brancheorganisationen Forbruger Elektronik
Business Software Alliance Danmark
Centralorganisationen af 2010 – CO10
Centralorganisationernes Fælles Udvalg
CSC Danmark A/S
Cybercity A/S
Dansk Arbejdsgiverforening
Dansk Erhverv

Dansk Industri (DI)
Dansk Internet Forum (DIFO)
Dansk IT
Dansk Journalistforbund
Dansk Kredit Råd,
Dansk Retspolitisk Forening
Danske Advokater
Danske Dagblades Forening
Danske Regioner
Datatilsynet
Deloitte
Den Danske Dommerforening
Det Kriminalpræventive Råd
DI ITEK
Digital Rights
Direktoratet for Kriminalforsorgen
DJØF
DKCERT
Dommerfuldmægtigforeningen
Domstolsstyrelsen
Erhvervs- og Vækstministeriet
Ernst & Young
Finansforbundet
Finansministeriet (Digitaliseringsstyrelsen)
Finansrådet
Forbrugerklagenævnet
Forbrugerombudsmanden
Forbrugerrådet Tænk
Foreningen af Danske Internet Medier
Foreningen af Offentlige Anklagere
Foreningen af Politimestre i Danmark
Foreningen af Statsadvokater
Forsikring og Pension
Forsvarets Efterretningstjeneste
Forsvarsministeriet (Center for Cybersikkerhed)
Funktionærernes og Tjenestemændenes Fællesråd
Hi3G Denmark ApS
HK Landsklubben Danmarks Domstole
HK Landsklubben for politiet
HORESTA
IFPI Danmark
Institut for Menneskerettigheder
ISP Sikkerhedsforum
ISPA DK (Foreningen af Internetleverandører)
IT-Brancheforeningen
ITEK
IT-Politisk Forening
IT-Sikkerhedsrådet
Justitsministeriet
Kommunale Tjenestemænd og Overenskomstansatte,

Kommunedata KMD
Kommunernes Landsforening (KL)
Konkurrencestyrelsen
Kontoret for politiforskning v/Politiskolen
KPMG
Kulturministeriet
Landbrug & Fødevarer
Landbrugsrådet
Landsforeningen af Beskikkede Advokater
Landsforeningen af Forsvarsadvokater
Professor i strafferet Jørn Vestergaard
Liberale Erhvervs Råd
LO
Lægemiddelindustriforeningen (LIF)
Lærernes Central Organisation
Multimedieforeningen
Offentligt Ansattes Organisationer
Telia A/S
PET
Politidirektøren i København
Politidirektørforeningen
Politiforbundet i Danmark
Politifuldmægtigforeningen
Procesbevillingsnævnet
Procesindustriens Brancheforening
PROSA
Præsidenten for Sø- og Handelsretten
Præsidenten for Vestre Landsret
Præsidenten for Østre Landsret
Præsidenten for Københavns Byret
Præsidenten for Århus byret
Præsidenten for Ålborg byret
Præsidenten for Odense byret
Præsidenten for Roskilde byret
Realkreditrådet
Retspolitisk Forening
Retssikkerhedsfonden
Rigsadvokaten
Rigspolitiet
Rigsrevisionen
Rådet for Digital Sikkerhed
SAM-DATA (HK)
Samtlige byretter
Sikkerhedsbranchen
Statens IT-Projektråd
Stats- og Kommunalt Ansattes Forhandlingsfællesskab
TDC A/S
Teknologirådet
Telekommunikationsindustrien (TI)
Telenor A/S

Telia A/S
The Open Web Application Security Project (OWASP
Danmark)
Torben Koch
Trine Baumbach
Økonomi- og Indenrigsministeriet (Afdeling for CPR-registre)

Bilag 3. Høringssvar

Samtlige høringssvar kan findes under Retsudvalgets dokumenter (alm. del. - bilag 364), på høringsportalen eller via følgende link:
<http://www.ft.dk/samling/20131/almudel/reu/bilag/364/index.htm#nav>