FOLKETINGSTIDENDE A

FOLKETINGET

Fremsat den 1. april 2016 af Rune Lund (EL) og Pernille Skipper (EL)

Forslag til folketingsbeslutning

om styrkelse af datasikkerhed

I forlængelse af beretning nr. 4 om datasikkerhed, som et enigt Retsudvalg afgav den 15. januar 2015, pålægger Folketinget regeringen inden den 1. januar 2017 at tage de nødvendige initiativer til at følge nedenstående anbefalinger m.v. fra beretningen (Beretning af almen art nr. 4 (2014-15 (1. samling)):

1) At der udarbejdes en årlig redegørelse om datasikkerhed til Folketinget.
2) At der oprettes en instans, som følger op på datasikkerhedsbrud, drager konklusioner på baggrund af bruddet, og som gør erfaringerne tilgængelige for øvrige myndigheder og virksomheder.
3) At indkalde Folketingets partier til politiske drøftelser med henblik på at sikre, at Datatilsynet tilføres de nødvendige ressourcer og beføjelser, så Datatilsynet og det effektive tilsyn med overholdelse af persondataloven styrkes.
4) At undersøge nærmere, hvordan Datatilsynet kan tilknyttes Folketinget i stedet for Justitsministeriet, og hvilke fordele der vil være forbundet hermed.
5) At fremsætte lovgivning, der sikrer, at offentlige myndigheder og private virksomheder gøres til genstand for samme sanktionsmuligheder.
6) At udrede, hvad databehandlers ansvar er i forhold til at sikre personoplysninger og overholde persondataloven, og hvordan databehandleres ansvar defineres i forhold til dataansvarliges ansvar.
7) At igangsætte de fornødne initiativer, herunder eventuelle lovgivningsinitiativer, så databehandler også gøres til pligtsubjekt i persondataretten.
8) At overveje det hensigtsmæssige i, at datasikkerhedsområdet fremover samles hos én ansvarlig minister. I den forbindelse skal det understreges, at Folketinget anerkender, at det er op til den siddende statsminister at foretage ændringer i ministeriernes ressortområder.
9) At inddrage princippet om privacy by design i fremtidige offentlige it-systemer. Desuden pålægges regeringen at tage de fornødne initiativer, så princippet om privacy by design bliver indført som et krav til samtlige leverandører af offentlige it- og digitaliseringsløsninger.
10) At de nuværende offentlige it-systemer opgraderes, så de nuværende it-systemerne lever op til principperne for privacy by design.
11) At implementeringen af ISO 27001 i statslige institutioner fremskyndes.
12) At opfølgning på kontrol med brugeradgange indskrives som krav i offentlige udbudskontrakter.
13) At der igangsættes en udredning af, om der bør være grænser for, hvad der kan gives samtykke til – og i så fald hvor grænserne for samtykke bør drages – på egne eller andres vegne i forhold til salg og udnyttelse af følsomme persondata.
14) At der foretages en kortlægning af eksisterende offentlige registre, og at det i forbindelse med kortlægningen overvejes, om der i nogle tilfælde registreres og opbevares mere data end nødvendigt.
15) At der udarbejdes en national strategi for informations- og datasikkerhed for den samlede offentlige sektor.
16) At brugen af cpr-nummeret bør gennemgå en grundlæggende revidering, herunder at opgivelse af cpr-nummer ikke alene skal kunne udgøre autentificering.

Bemærkninger til forslaget

Generelle bemærkninger

Forslagsstillerne ønsker at følge op på beretningen om datasikkerhed, som et enigt Retsudvalg afgav torsdag den 15. januar 2015 (Beretning af almen art nr. 4 (2014-15 (1. samling)).

Justitsministeren har efterfølgende på regeringens vegne kommenteret beretningen i svar af 14. januar 2016 på Retsudvalgets spørgsmål nr. 147 af 31. august 2015, hvor justitsministeren bliver bedt om at kommentere beretningen og redegøre for, hvilke initiativer ministeren på baggrund af beretningen agter at tage.

I sit svar oplyser justitsministeren bl.a., at Justitsministeriet i samarbejde med andre ministerier i 2014 blev bedt om at kortlægge beskyttelsen af oplysninger om borgernes elektroniske betalinger m.v., og at dette arbejde forventes afsluttet inden udgangen af februar 2016. Kortlægningen skal danne udgangspunkt for en bred politisk drøftelse.

Justitsministeren indledte på et møde den 16. september 2014 en politisk drøftelse, bl.a. om en samlet strategi til sikring af danskernes personoplysninger. På mødet blev det aftalt at fortsætte møderækken, så snart kortlægningsarbejdet er afsluttet.

Forslagsstillerne ønsker med forslaget at sikre fortsat politisk opbakning til og opmærksomhed om anbefalingerne i beretningen og sikre, at de tiltag, som et enigt Retsudvalg besluttede at bakke op om, føres ud i livet.

Bemærkninger til forslagets enkelte punkter

Bemærkningerne til de enkelte punkter nedenfor er en gengivelse af bemærkningerne fra beretningen.

Til nr. 1

1) At der udarbejdes en årlig redegørelse om datasikkerhed til Folketinget.

Af indledningen i beretningen fremgår:

»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 til, jf. REU alm. del – svar på spørgsmål 1240, folketingsåret 2013-14.«

Til nr. 2

2) At der oprettes en instans, som følger op på datasikkerhedsbrud, drager konklusioner på baggrund af bruddet, og som gør erfaringerne tilgængelige for øvrige myndigheder og virksomheder.

Dette er et af de principper, som arbejdsgruppen opstillede, og som fremgår af beretningens politiske bemærkninger under afsnit 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.«

Til nr. 3

3) At indkalde Folketingets partier til politiske drøftelser med henblik på at sikre, at Datatilsynet tilføres de nødvendige ressourcer og beføjelser, så Datatilsynet og det effektive tilsyn med overholdelse af persondataloven styrkes.

Af beretningens politiske bemærkninger under afsnit 3.2 Tilsynet med overholdelse af persondataloven fremgår:

»*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 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.«

Til nr. 4

4) At undersøge nærmere, hvordan Datatilsynet kan tilknyttes Folketinget i stedet for Justitsministeriet, og hvilke fordele der vil være forbundet hermed.

Af beretningens politiske bemærkninger under afsnit 3.2 Tilsynet med overholdelse af persondataloven fremgår:

»*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.«

Til nr. 5

5) At fremsætte lovgivning, der sikrer, at offentlige myndigheder og private virksomheder gøres til genstand for samme sanktionsmuligheder.

Af beretningens politiske bemærkninger under afsnit 3.3 Øgede sanktionsmuligheder ved brud på datasikkerhed fremgår:

»*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.«

Til nr. 6 og 7

6) At udrede, hvad databehandlers ansvar er i forhold til at sikre personoplysninger og overholde persondataloven, og hvordan databehandleres ansvar defineres i forhold til dataansvarliges ansvar.

7) At igangsætte de fornødne initiativer, herunder eventuelle lovgivningsinitiativer, så databehandler også gøres til pligtsubjekt i persondataretten.

Af beretningens politiske bemærkninger under afsnit 3.3 Øgede sanktionsmuligheder ved brud på datasikkerhed fremgår:

»*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 – 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.«

Til nr. 8

8) At overveje det hensigtsmæssige i, at datasikkerhedsområdet fremover samles hos én ansvarlig minister. I den forbindelse skal det understreges, at Folketinget anerkender, at det er op til den siddende statsminister at foretage ændringer i ministeriernes ressortområder.

Af beretningens politiske bemærkninger under afsnit 3.4 Samling af ansvaret for datasikkerhed fremgår:

»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.«

Til nr. 9 og 10

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

10) At de nuværende offentlige it-systemer opgraderes, så de nuværende it-systemerne lever op til principperne for privacy by design.

Af beretningens politiske bemærkninger under afsnit 3.5 Tekniske krav til sikring af følsomme fortrolige personoplysninger fremgår:

»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.«

Til nr. 11

11) At implementeringen af ISO 27001 i statslige institutioner fremskyndes.

Af beretningens politiske bemærkninger under afsnit 3.5 Tekniske krav til sikring af følsomme fortrolige personoplysninger fremgår:

»*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.«

Til nr. 12

12) At opfølgning på kontrol med brugeradgange indskrives som krav i offentlige udbudskontrakter.

Af beretningens politiske bemærkninger under afsnit 3.5 Tekniske krav til sikring af følsomme fortrolige personoplysninger fremgår:

»*Kontrol af rollebaseret adgang*

Af sikkerhedsbekendtgørelsen § 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.«

Til nr. 13-16

13) At der igangsættes en udredning af, om der bør være grænser for, hvad der kan gives samtykke til – og i så fald hvor grænserne for samtykke bør drages – på egne eller andres vegne i forhold til salg og udnyttelse af følsomme persondata.

14) At der foretages en kortlægning af eksisterende offentlige registre, og at det i forbindelse med kortlægningen overvejes, om der i nogle tilfælde registreres og opbevares mere data end nødvendigt.

15) At der udarbejdes en national strategi for informations- og datasikkerhed for den samlede offentlige sektor.

16) At brugen af cpr-nummeret bør gennemgå en grundlæggende revidering, herunder at opgivelse af cpr-nummer ikke alene skal kunne udgøre autentificering.

Af beretningens politiske bemærkninger under afsnit 3.6 Øvrige bemærkninger fremgår:

»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.«

Skriftlig fremsættelse

Pernille Skipper (EL):

Som ordfører for forslagsstillerne tillader jeg mig herved at fremsætte:

Forslag til folketingsbeslutning om styrkelse af datasikkerhed.

(Beslutningsforslag nr. B 148)

Jeg henviser i øvrigt til de bemærkninger, der ledsager forslaget, og anbefaler det til Tingets velvillige behandling.