FOLKETINGSTIDENDE B

FOLKETINGET

Betænkning afgivet af Transport-, Bygnings- og Boligudvalget den 24. april 2018

Betænkning

over

Forslag til lov om sikkerhed i net- og informationssystemer i transportsektoren

[af transport-, bygnings- og boligministeren (Ole Birk Olesen)]

1. Ændringsforslag

Transport-, bygnings- og boligministeren har stillet 2 ændringsforslag til lovforslaget.

2. Udvalgsarbejdet

Lovforslaget blev fremsat den 7. februar 2018 og var til 1. behandling den 20. februar 2018. Lovforslaget blev efter 1. behandling henvist til behandling i Transport-, Bygnings- og Boligudvalget.

Møder

Udvalget har behandlet lovforslaget i 4 møder.

Sammenhæng med andre lovforslag

Lovforslaget skal ses i sammenhæng med lovforslag nr. 139 (Lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.) og lovforslag nr. 155 (Konsekvensændringer som følge af databeskyttelsesforordningen og databeskyttelsesloven), som begge er behandlet i Forsvarsudvalget, lovforslag nr. 143 (Lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren), som er behandlet i Sundheds- og Ældreudvalget, og L 144 (Lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester), som er behandlet i Erhvervs-, Vækst- og Eksportudvalget.

Høring

Et udkast til lovforslaget har inden fremsættelsen været sendt i høring. Den 9. februar 2018 sendte transport-, bygnings- og boligministeren de indkomne høringssvar og et notat herom til udvalget.

Teknisk gennemgang

Forsvarsministeren afholdt den 14. marts 2018 en teknisk gennemgang af Center for Cybersikkerheds rolle i forbindelse med implementering af NIS-direktivet. Transport-, bygnings- og boligministeren afholdt den 15. marts 2018 en teknisk gennemgang af lovforslaget, for så vidt angår ministerens ressortområde vedrørende implementeringen af NIS-direktivet.

Spørgsmål

Udvalget har stillet 12 spørgsmål til transport-, bygnings- og boligministeren og forsvarsministeren til skriftlig besvarelse, som disse har besvaret.

Fem af udvalgets spørgsmål til transport-, bygnings- og boligministeren og forsvarsministeren og disses svar herpå er optrykt som bilag 2 til betænkningen.

3. Indstillinger og politiske bemærkninger

Et *flertal* i udvalget (S, DF, V, LA, RV og KF) indstiller lovforslaget til *vedtagelse* med de stillede ændringsforslag.

Socialdemokratiets medlemmer af udvalget er stærkt optaget af at sikre så meget beskyttelse af og sikkerhed for vores vitale it-infrastruktur. Danmark skal selvsagt gardere sig så meget som muligt imod cyberangreb, spionage, manipulation og terror m.v. Etablering af nationale kontaktpunkter er derfor et fornuftigt og nødvendigt tiltag.

Socialdemokratiet er imidlertid betænkelige ved, at den nye indsats kan komme til at skade persondatabeskyttelsen, ligesom Socialdemokratiet i udvalgsbehandlingen har ytret betænkelighed ved, at ordningen kan blive særdeles bekostelig og bureaukratisk for de berørte enheder, der skal underlægges de nye og måske temmelig dyre krav.

Socialdemokratiet ønsker derfor de stillede spørgsmål og svar vedrørende disse emner optrykt i betænkningen. Socialdemokratiet ønsker at følge lovens implementering og udmøntning af loven særdeles tæt. Socialdemokratiet opfordrer Transport-, Bygnings- og Boligministeriet til løbende at orientere Transport-, Bygnings- og Boligudvalget om udviklingen på området – navnlig med henblik på de nævnte problemstillinger. Udvalget bør orienteres løbende, så processen følges tæt.

Dansk Folkepartis medlemmer af udvalget støtter naturligvis intentionerne med bedre sikkerhed i net- og informationssystemer i transportsektoren, men er betænkelige ved, at udvalget ikke kan få oplyst omfanget af den organisation, der skal varetage dette, og hvordan der skal differentieres mellem operatører af væsentlige og ikkevæsentlige transporttjenester, og altså hvem der bliver omfattet.

Et *mindretal* i udvalget (EL, SF og ALT) vil stemme hverken for eller imod lovforslaget ved 3. behandling. Mindretallet vil stemme for de stillede ændringsforslag.

Enhedslistens, Socialistisk Folkepartis og Alternativets medlemmer af udvalget bemærker, at det er vigtigt, at vi styrker beskyttelsen af vores vitale infrastruktur mod cyberangreb, og etablering af nationale kontaktpunkter er derfor et fornuftigt tiltag. Imidlertid er mindretallet bekymrede over, at CSIRT'en og det nationale kontaktpunkt, som skal oprettes i medfør af NIS-direktivet, placeres under Center for Cybersikkerhed under Forsvarets Efterretningstjeneste og dermed ikke omfattes af relevante love for bl.a. persondatabeskyttelse.

Mindretallet mener, at Center for Cybersikkerheds aktiviteter i medfør af NIS-direktivet bør omfattes af databeskyttelsesloven og databeskyttelsesforordningen. Det fremgår også tydeligt af NIS-direktivet, at det er hensigten. Og derfor har mindretallet således stillet et ændringsforslag til lovforslag nr. L 155, der skal sikre dette.

Inuit Ataqatigiit, Tjóðveldi og Javnaðarflokkurin var på tidspunktet for betænkningens afgivelse ikke repræsenteret med medlemmer i udvalget og havde dermed ikke adgang til at komme med indstillinger eller politiske udtalelser i betænkningen.

En oversigt over Folketingets sammensætning er optrykt i betænkningen.

4. Ændringsforslag med bemærkninger

Ændringsforslag

Af *transport-, bygnings- og boligministeren,* tiltrådt af *udvalget:*

Til § 13

1) I *stk. 1* ændres »den, der« til: »den operatør, der«.
[Præcisering]

2) I *stk. 1, nr. 1,* ændres »som de leverer« til: »som operatøren leverer«.
[Præcisering]

Bemærkninger

Til nr. 1

Der er tale om en sproglig præcisering, således at det tydeliggøres, at det er operatøren, der kan straffes.

Til nr. 2

Der er tale om en sproglig præcisering, således at det tydeliggøres, at det er operatøren, der leverer de væsentlige transporttjenester.

Kim Christiansen (DF) nfmd. *Per Nørhave (DF) Claus Kvist Hansen (DF) Mette Hjermind Dencker (DF)*

Jan Erik Messmann (DF) Henrik Brodersen (DF) Kristian Pihl Lorentzen (V) Hans Andersen (V)

Hans Christian Schmidt (V) Jane Heitmann (V) Louise Schack Elholm (V) Britt Bager (V) May-Britt Kattrup (LA)

Villum Christensen (LA) Rasmus Jarlov (KF) Christian Rabjerg Madsen (S) Erik Christensen (S) Kaare Dybvad (S)

Lennart Damsbo-Andersen (S) fmd. *Magnus Heunicke (S) Rasmus Prehn (S) Mette Reissmann (S) Daniel Toft Jakobsen (S)*

Henning Hyllested (EL) Søren Egge Rasmussen (EL) Roger Courage Matthisen (ALT) Andreas Steenberg (RV)

Karsten Hønge (SF) Kirsten Normann Andersen (SF)

Inuit Ataqatigiit, Tjóðveldi og Javnaðarflokkurin havde ikke medlemmer i udvalget.

Socialdemokratiet (S)	46	Socialistisk Folkeparti (SF)	7
Dansk Folkeparti (DF)	37	Det Konservative Folkeparti (KF)	6
Venstre, Danmarks Liberale Parti (V)	34	Inuit Ataqatigiit (IA)	1
Enhedslisten (EL)	14	Tjóðveldi (T)	1
Liberal Alliance (LA)	13	Javnaðarflokkurin (JF)	1
Alternativet (ALT)	10	Uden for folketingsgrupperne (UFG)	1
Radikale Venstre (RV)	8		

Bilag 1

Oversigt over bilag vedrørende L 135

Bilagsnr.	Titel
1	Høringssvar og høringsnotat, fra transport-, bygnings- og boligministeren
2	Udkast til tidsplan for udvalgets behandling af lovforslaget
3	Tidsplan for udvalgets behandling af lovforslaget
4	Notat i forlængelse af den tekniske gennemgang af Center for Cybersikkerheds rolle i forbindelse med implementering af NIS-direktivet, fra forsvarsministeren
5	Revideret tidsplan for udvalgets behandling af lovforslaget
6	Trafik-, Bygge- og Boligstyrelsens præsentation fra den tekniske gennemgang den 15/3-18
7	Ændringsforslag fra transport-, bygnings- og boligministeren
8	Præsentation fra den tekniske gennemgang af Center for Cybersikkerheds rolle i forbindelse med implementering af NIS-direktivet, fra forsvarsministeren
9	Udkast til betænkning
10	Revideret tidsplan for udvalgets behandling af lovforslaget

Oversigt over spørgsmål og svar vedrørende L 135

Spm.nr.	Titel
1	Spm. om, hvorfor der med lovforslaget lægges op til, at hændelser kan deles/offentliggøres, hvis særlige omstændigheder er til stede, i stedet for at gøre det til en pligt at dele/offentliggøre hændelser, medmindre særlige omstændigheder er til stede, til transport-, bygnings- og boligministeren, og ministerens svar herpå
2	Spm., om Center for Cybersikkerhed i Forsvarets Efterretningstjeneste, når det løser opgaver i regi af lovforslaget som nationalt centralt kontaktpunkt og CSIRT, er omfattet af eller undtaget fra forslaget om en ny databeskyttelseslov (L 68), persondataforordningen, offentlighedsloven og forvaltningsloven, til transport-, bygnings- og boligministeren og forsvarsministeren, og ministrenes svar herpå
3	Spm., om Center for Cybersikkerhed i regi af lovforslaget skal forstås som en forvaltningsmyndighed, jf. forvaltningsloven, til transport-, bygnings- og boligministeren og forsvarsministeren, og ministrenes svar herpå
4	Spm. om, hvorledes beskyttelsen af personoplysninger i gennemførelsen af NIS-direktivet kan leve op til kravet i direktivets artikel 2 samt artikel 8 i EU's charter for grundlæggende rettigheder, til transport-, bygnings- og boligministeren og forsvarsministeren, og ministrenes svar herpå
5	Spm. om ministerens kommentar til høringssvaret fra Institut for Menneskerettigheder, til transport-, bygnings- og boligministeren og forsvarsministeren, og ministrenes svar herpå

6 Spm. om, hvilke data det forventes at operatører af væsentlige transporttjenester vil skulle indberette til ministeren og Center for Cybersikkerhed i tilfælde af en såkaldt hændelse, til transport-, bygnings- og boligministeren og forsvarsministeren, og ministrenes svar herpå

7 Spm., om ministeren kan be- eller afkræfte, om der vil være en chance for, at personoplysninger fra eksempelvis rejsekort m.v. vil kunne komme til at indgå i de indberettede oplysninger fra operatører af væsentlige transporttjenester til ministeren og Center for Cybersikkerhed, til transport-, bygnings- og boligministeren og forsvarsministeren, og ministrenes svar herpå

8 Spm. om, hvilke konkrete oplysninger det forventes at ministeren og Center for Cybersikkerhed vil kunne eller skulle udveksle med andre myndigheder både nationalt og i EU, til transport-, bygnings- og boligministeren og forsvarsministeren, og ministerenes svar herpå

9 Spm. om, hvordan de andre EU-lande har valgt at organisere gennemførelsen af NIS-direktivet, til forsvarsministeren, kopi til transport-, bygnings- og boligministeren, og ministerens svar herpå

10 Spm., om ministeren vil uddybe baggrunden for vurderingen af, at lovforslaget kun vil få mindre økonomiske og administrative konsekvenser for de berørte offentlige og private operatører af væsentlige transporttjenester, til transport-, bygnings- og boligministeren, og ministerens svar herpå

11 Spm. om, hvilken nedre grænse der forventes i forbindelse med udpegning af operatører af væsentlige transporttjenester, til transport-, bygnings- og boligministeren, og ministerens svar herpå

12 Spm. om en redegørelse for regeringens holdning til de stillede ændringsforslag til lovforslag nr. L 155, til transport-, bygnings- og boligministeren og forsvarsministeren, og ministrenes svar herpå

Bilag 2

Fem af udvalgets spørgsmål til transport-, bygnings- og boligministeren og forsvarsministeren og disses svar herpå

Spørgsmålene og svarene er optrykt efter ønske fra S.

Spørgsmål 2:

Ministeren bedes redegøre for, om Center for Cybersikkerhed i Forsvarets Efterretningstjeneste, når det løser opgaver i regi af lovforslaget som nationalt centralt kontaktpunkt og CSIRT, er omfattet eller undtaget af forslaget om en ny databeskyttelseslov (L 68), persondataforordningen, offentlighedsloven og forvaltningsloven. Herunder ønskes oplyst, hvilke konkrete dele af lovene og forordningen, som Center for Cybersikkerhed vil være omfattet af/ikke omfattet af.

Svar:

Der henvises til den samtidige besvarelse af spørgsmål nr. 3 vedrørende L 135.

Spørgsmål 3:

På baggrund af afsnit 3 i de almindelige bemærkninger til lovforslaget bedes ministeren oplyse, om Center for Cybersikkerhed i regi af lovforslaget skal forstås som en forvaltningsmyndighed, jf. forvaltningsloven. Ministeren bedes i forlængelse heraf redegøre for kravene til centerets behandling af personoplysninger. Herunder ønskes oplyst, hvorledes kravene adskiller sig som følge af reglerne i lov om Center for Cybersikkerhed (lov nr. 713 af 25. juni 2014), set i forhold til databeskyttelsesforordningen (forordning 2016/679/EU af 27. april 2016 om beskyttelse af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF) samt forslaget til databeskyttelseslov (L 68), hvis Forsvarets Efterretningstjeneste ikke er omfattet af lovforslaget og forordningen.

Svar:

1. Det følger af § 8 i lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, at Center for Cybersikkerheds virksomhed er undtaget fra offentlighedsloven (bortset fra lovens § 13 om notatpligt) og forvaltningslovens kapitel 4-6. Dette gælder også for centerets kommende funktioner som nationalt centralt kontaktpunkt og CSIRT efter NIS-direktivet (Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen).

Det fremgår dog af bemærkningerne til forslaget til lov om Center for Cybersikkerhed (L 192, fremsat 2. maj 2014), at Center for Cybersikkerhed forudsættes i videst muligt omfang at efterleve principperne i offentlighedsloven og forvaltningslovens kapitel 4-6. Det forudsættes således, at centeret – uanset at dets virksomhed er undtaget fra forvaltningslovens bestemmelser på området – i alle afgørelsessager konkret vurderer, om det er muligt at anvende forvaltningslovens principper om partens aktindsigt, partshøring og begrundelse m.v. Tilsvarende forudsættes det, at anmodninger om aktindsigt i videst muligt omfang behandles efter principperne i offentlighedsloven.

Det bemærkes i den forbindelse, at Center for Cybersikkerheds afgørelser i konkrete sager, f.eks. aktindsigtssager, kan påklages til Forsvarsministeriet.

2. Center for Cybersikkerheds virksomhed, herunder centerets kommende funktioner efter NIS-direktivet, er endvidere undtaget fra persondataloven. Denne retstilstand ventes videreført, når persondataloven med virkning fra 25. maj 2018 erstattes af databeskyttelsesforordningen (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF) og den foreslåede databeskyttelseslov (L 68, fremsat for Folketinget den 25. oktober 2017).

Størstedelen af de centrale principper i persondataloven gælder dog for centeret, jf. kapitel 6 i lov om Center for Cybersikkerhed. Det følger således bl.a. af loven, at centeret kun må indsamle personoplysninger til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål. Endvidere må centeret ikke behandle flere personoplysninger, end hvad der kræves til opfyldelse af formålet med indsamlingen. Der stilles desuden krav om hjemmel til enhver behandling af personoplysninger, ligesom der som udgangspunkt ikke må behandles personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning og fagforeningsmæssige tilhørsforhold samt personoplysninger om helbredsmæssige og seksuelle forhold. Centeret skal derudover sikre, at der ikke behandles urigtige eller vildledende personoplysninger. Endelig må centeret ikke opbevare indsamlede personoplysninger på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end nødvendigt, og centeret skal træffe passende sikkerhedsforanstaltninger ved behandlingen af personoplysninger.

Visse centrale krav efter persondataloven gælder dog ikke for Center for Cybersikkerhed. Centeret er således undtaget fra kravet om oplysningspligt overfor den registrerede samt kravet om den registreredes indsigts- og indsigelsesret.

Herudover er det Tilsynet med Efterretningstjenesterne – og ikke Datatilsynet – der fører tilsyn med Center for Cybersikkerheds behandling af personoplysninger. Tilsynet med Efterretningstjenesterne er et uafhængigt kontrolorgan, der efter klage eller af egen drift påser, at Center for Cybersikkerhed overholder reglerne vedrørende behandling af personoplysninger.

3. Endvidere følger det af § 8, stk. 2, i lov om Center for Cybersikkerhed, at forsvarsministeren kan bestemme, at kapitel 8-10 i persondataloven, kapitel 4-6 i forvaltningsloven samt offentlighedsloven helt eller delvist skal finde anvendelse for Center for Cybersikkerheds virksomhed som bl.a. myndighed for informationssikkerhed og beredskab på teleområdet.

Der har indtil videre ikke vist sig behov for at anvende denne bemyndigelse, idet der behandles ganske få personoplysninger i forbindelse med centerets virksomhed på teleområdet.

Med lovforslag L 155 om ændring af lov om Center for Cybersikkerhed, der er fremsat for Folketinget den 28. februar 2018, foreslås det bl.a., at den nævnte bemyndigelse tilpasses til den kommende regulering på databeskyttelsesområdet og NIS-området, således at forsvarsministeren vil kunne bestemme, at databeskyttelsesforordningen og den foreslåede databeskyttelseslov også helt eller delvist skal finde anvendelse for de myndighedsopgaver, som Center for Cybersikkerhed tillægges som led i implementeringen af NIS-direktivet.

4. Blandt de nye krav, som databeskyttelsesforordningen stiller, kan fremhæves krav om udpegelse af en databeskyttelsesrådgiver, at der skal gennemføres konsekvensanalyser, og at nye systemer skal have indbygget databeskyttelse (privacy by design or by default).

For en nærmere gennemgang af forholdet mellem databeskyttelsesforordningen og persondataloven henvises i øvrigt til Justitsministeriets betænkning nr. 1565 om databeskyttelsesforordningen, del I, bind 1.

Spørgsmål 4:

Ministeren bedes redegøre for, hvorledes beskyttelsen af personoplysninger i gennemførelsen af NIS-direktivet (direktiv 2106/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen) kan leve op til kravet i direktivets artikel 2 samt artikel 8 i EU's charter for grundlæggende rettigheder.

Svar:

Det følger af artikel 2, stk. 1, i NIS-direktivet (Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen), at behandlingen af personoplysninger efter direktivet udføres i overensstemmelse med databeskyttelsesdirektivet (Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger).

Databeskyttelsesdirektivet gælder bl.a. ikke for sådan behandling af personoplysninger, der vedrører statens sikkerhed, jf. direktivets artikel 3, stk. 2. På den baggrund gælder den danske persondatalov – der implementerer databeskyttelsesdirektivet i dansk ret – heller ikke for behandlinger af personoplysninger, der udføres for Forsvarets Efterretningstjeneste, herunder Center for Cybersikkerhed.

En række af de centrale bestemmelser i persondataloven er imidlertid indarbejdet i lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, der regulerer centerets virksomhed. Endvidere fører Tilsynet med Efterretningstjenesterne, som er et uafhængigt kontrolorgan, tilsyn med Center for Cybersikkerheds behandling af personoplysninger. Tilsynet kan hos Center for Cybersikkerhed kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed. Man kan som borger klage til tilsynet, hvis man mener, at centeret ulovligt behandler personoplysninger om en. Tilsynet afgiver endvidere hvert år en redegørelse til forsvarsministeren om tilsynets virksomhed i forhold til Center for Cybersikkerhed, og redegørelsen offentliggøres.

Denne retstilstand videreføres som udgangspunkt, når EU's databeskyttelsesdirektiv fra 25. maj 2018 erstattes af den nye databeskyttelsesforordning (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF) samt den foreslåede danske databeskyttelseslov (L 68, fremsat for Folketinget den 25. oktober 2017).

Det bemærkes dog, at der med lovforslag nr. L 155, der konsekvensændrer lov om Center for Cybersikkerhed som følge af den nye regulering på databeskyttelsesområdet, er lagt op til, at forsvarsministeren får hjemmel til helt eller delvist at sætte databeskyttelsesforordningen og databeskyttelsesloven i kraft for dele af Center for Cybersikkerheds virksomhed, herunder centerets virksomhed i medfør af NIS-direktivet. Dette lovforslag blev fremsat den 28. februar 2018 og er fortsat under behandling i Folketinget.

Spørgsmål 5:

Ministeren bedes kommentere høringssvaret fra Institut for Menneskerettigheder, herunder særligt instituttets bekymring for det principielt problematiske i, at centrale civile samfundsstrukturer i Danmark skal varetages af Forsvarets Efterretningstjeneste med de begrænsninger, det giver i forhold til indsigt i databeskyttelseskrav.

Svar:

1. Institut for Menneskerettigheder fremfører i instituttets høringssvar, at instituttet anser det for principielt problematisk, at implementeringen af NIS-direktivet medfører, at stadig flere oplysninger bliver udvekslet med Center for Cybersikkerhed, der er en del af Forsvarets Efterretningstjeneste, ligesom instituttet finder det problematisk, at centeret er undtaget fra bl.a. persondataloven.

2. NIS-direktivet forpligter medlemsstaterne til at udpege et nationalt centralt kontaktpunkt. Det nationale centrale kontaktpunkt skal udgøre et forbindelsesled, som faciliterer det grænseoverskridende samarbejde med andre medlemsstater, netværket af it-beredskabsenheder (CSIRT'er) og den samarbejdsgruppe, som skal have fokus på det strategiske samarbejde om sikkerhed i net- og informationssystemer mellem medlemsstaterne. Herudover skal det centrale kontaktpunkt én gang om året forelægge en sammenfattende rapport for samarbejdsgruppen vedrørende underretninger om hændelser i henhold til NIS-direktivet.

Center for Cybersikkerhed er i forvejen national it-sikkerhedsmyndighed og står for en forebyggende rådgivnings- og oplysningsvirksomhed om cybersikkerhed i forhold til både den offentlige og private sektor samt en reaktiv indsats ved cyberangreb. Center for Cybersikkerhed varetager en række myndighedsopgaver i den forbindelse, og centeret er således allerede den centrale nationale myndighed vedrørende cybersikkerhed. På den baggrund vil varetagelsen af funktionen som nationalt centralt kontaktpunkt ligge i naturlig forlængelse af centerets øvrige opgaver.

3. NIS-direktivet forpligter herudover medlemsstaterne til at udpege en eller flere nationale CSIRT'er. En CSIRT skal fungere som national beredskabsenhed til håndtering af it-sikkerhedshændelser og vil bl.a. have til opgave at foretage monitorering af hændelser på nationalt plan, udsende tidlige varslinger, advarsler og meddelelser samt formidle information til relevante interessenter om risici og hændelser. CSIRT'en vil endvidere skulle reagere på hændelser og udarbejde dynamiske risiko- og hændelsesanalyser samt situationsrapporter. Endelig vil CSIRT'en skulle deltage i det føromtalte CSIRT-netværk og etablere samarbejde med den private sektor.

Center for Cybersikkerhed besidder allerede i dag mange af de kompetencer, der er nødvendige for at kunne varsle sektorerne samt reagere på hændelser, og centeret vil tillige kunne operere døgnet rundt. CSIRT-funktionen efter NIS-direktivet har således en nær sammenhæng med Center for Cybersikkerheds eksisterende opgaver.

4. Center for Cybersikkerhed og den øvrige del af FE er – selvom de udgør én myndighed – ved lov tillagt forskellige opgaver og virkemidler. Center for Cybersikkerhed er særskilt reguleret i lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, hvor der i bemærkningerne er forudsat en vis organisatorisk adskillelse mellem centeret og den efterretningsmæssige del af FE. Det er også forudsat, at centeret har en åben og udadvendt profil, og at centerets virksomhed skal være præget af åbenhed, vejledning og information.

For en nærmere beskrivelse af kravene til Center for Cybersikkerheds behandling af personoplysninger henvises der i øvrigt til den samtidige besvarelse af spørgsmål 3 vedrørende L 135.

Spørgsmål 10:

Ministeren bedes uddybe baggrunden for vurderingen af, at lovforslaget kun vil få mindre økonomiske og administrative konsekvenser for de berørte offentlige og private operatører af væsentlige transporttjenester. Dette da det ikke umiddelbart ses at fremgå af høringssvar eller høringsnotat, hvordan eksempelvis Københavns Lufthavn, DSB, Banedanmark eller Naviair vurderer lovforslagets konsekvenser.

Svar:

Indledningsvist skal jeg bemærke, at de nævnte operatører alle har været hørt over lovforslaget.

Det er min forventning, at der alene vil blive udpeget nogle ganske få private og offentlige aktører, som alle vil være karakteriseret ved at være særdeles store operatører, der alle leverer en unik tjeneste inden for hver deres område, som er afhængige af IT-systemer og som har en transportmæssig kritisk og national betydning for hvert deres område.

Kravet om, at en operatør af væsentlige transporttjenester skal være certificeret i henhold til en internationalt anerkendt standard, skønnes afhængigt af certificeringsparatheden hos den enkelte operatør at udgøre op til 200.000 kr. i direkte engangsomkostninger og 40.000-100.000 kr. i direkte årlige vedligeholdelsesomkostninger til selve certificeringen. Hvis der er tale om en operatør, der ikke er certificeringsparat, og som har brug for at gennemføre tilpasninger af net- og informationssystemer m.m., vil omkostningerne for den enkelte operatør kunne være større, afhængigt af hvor meget der udestår for operatøren for at kunne opnå den efterspurgte certificering.

Lovforslagets certificeringsmodel har sideløbende med udarbejdelsen af lovforslaget været drøftet med Københavns Lufthavn, DSB og Naviair. Disse operatører følger i vidt omfang allerede i dag en internationalt anerkendt standard for sikkerheden i net- og informationssystemer. Det gør de, fordi standarden giver en systematisk og tidssvarende tilgang til at styre de risici, der er ved at være afhængig af net- og informationssystemer. Disse operatører har alle selv en interesse i, at de har en robusthed i forhold til at kunne levere den ydelse, de lever af, og at de kan levere den uden væsentlige forsinkelser og gener.

De nævnte operatører har derfor allerede i dag indrettet deres virksomheder, så de i vidt omfang efterlever de internationale standarder. Det vil derfor ikke være fremmed for disse operatører at lade sig certificere i henhold til en international standard.

I henhold til regeringens nationale strategi for cyber- og informationssikkerhed fra december 2014 har BaneDanmark, som alle statslige myndigheder siden 2016, været forpligtet til at implementere den internationale sikkerhedsstandard ISO27001.

Det vurderes, at de operatører, der vil kunne komme i betragtning til en udpegning efter loven, i et eller andet omfang er certificeringsparate. Operatørerne vil endvidere alle være af en ganske betydelig størrelse. Ud fra en forholdsmæssig betragtning forventer jeg derfor ikke, at de foreslåede regler vil blive oplevet som meget bebyrdende for operatørerne af væsentlige transporttjenester.

Ud over omkostningerne til certificering og vedligeholdelse heraf vil der være begrænsede administrative byrder i forbindelse med den underretning, som operatørerne skal sende til myndighederne. Det forventes, at der vil være et begrænset antal underretninger fra den enkelte operatør på årsbasis. Selve den administrative håndtering af underretningen forventes ikke at overstige 2 timer pr. hændelse.