

HØRINGSNOTAT VEDR. FORSLAG TIL LOV OM SIKKERHED I NET- OG INFORMATIONSSYSTEMER I TRANSPORTSEKTOREN

Dato 8. februar 2018
J. nr. 2017-4685

I. Høringen

Udkast til forslag til lov om sikkerhed i net- og informationssystemer i transportsektoren har været sendt i høring fra onsdag den 29. november 2017 til tirsdag den 2. januar 2018. Desuden har lovudkastet været i offentligt tilgængeligt på høringsportalen (<https://hoeringsportalen.dk/>) i hele høringsperioden.

Transport-, Bygnings-, og Boligministeriet har modtaget høringssvar fra:

Danske Havne, Danske Rederier, Danske Regioner, Datatilsynet, DB Cargo Scandinavia A/S, DSB, Erhvervsflyvningens Sammenslutning, Færge Rederierne, Institut for Menneskerettigheder, IT-Politisk Forening, Naviair, Rederiforeningen, Rigsrevisionen, Trafikselskaberne og Øresundsbro Konsortiet.

DB Cargo Scandinavia A/S, Naviair og Rigsrevisionen har meddelt, at de ikke har bemærkninger til lovforslaget.

Nedenfor er angivet de væsentligste punkter i de modtagne høringssvar. Transport-, Bygnings- og Boligministeriets bemærkninger til høringssvarene er anført med *kursiv*.

II. Høringssvar

1. *Generelle bemærkninger*

IT-Politisk Forening vurderer, at den valgte sektoropdeling med flere kompetente myndigheder kan sprede tilsynsressourcerne mere, end hvad godt er, og synergieffekterne mellem forskellige tilsynsmyndigheder kan blive vanskelige at udnytte.

Der er stor forskel på de sektorer, der er omfattet af direktivet. Målet med sektoropdelingen er, at lovgivningen tilpasses den enkelte sektor for derved at opnå den bedst mulige beskyttelse af net- og informationssystemer og samtidig sikre, at erhvervslivet ikke pålægges unødvendige byrder. Ved implementeringen af NIS-direktivet videreføres sektoransvaret derfor, således at de enkelte ressortmyndigheder inden for eget område har ansvaret for at fastsætte og håndhæve reglerne om informationssikkerhed.



2. Definitioner

DSB anfører, at definitionerne i lovforslaget kunne være mere præcist formuleret, så bl.a. scopet for lovforslaget og afgrænsninger i forhold til systemer omfattet af lovforslaget tydeliggøres.

Lovforslagets definitioner bygger på de tilsvarende definitioner i NIS-direktivets art. 4. Definitionerne skal læses i sammenhæng med de øvrige bestemmelser i lovforslaget.

Lovforslaget stiller alene krav om, at operatøren skal træffe foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer for så vidt angår den del af en operatørs aktiviteter, hvor en hændelse vil få en væsentlig forstyrrende virkning for leveringen af en transporttjeneste.

Lovforslaget giver hjemmel til, at transport-, bygnings- og boligministeren fastsætter nærmere regler i en bekendtgørelse. De nærmere regler vil eksempelvis være en tydeliggørelse af, hvad der kvalificeres som væsentlige tjenester inden for dele af transportsektoren. Herudover vil der være nærmere regler om de foranstaltninger, der skal træffes for at styre risiciene for sikkerheden i net- og informationssystemerne og for at forebygge og minimere konsekvenserne af hændelser, der kan have negativ indvirkning på sikkerheden i de anvendte net- og informationssystemer.

IT-Politisk Forening bemærker, at ansvaret for de tværgående opgaver som følge af NIS-direktivet ikke er omtalt i lovforslagets bemærkninger.

Transport-, Bygnings- og Boligministeriet har præciseret i lovforslaget, at underretningerne retteligt skal ske til den nationale it-beredskabsenhed, der håndterer hændelser, og som har ansvaret for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU (CSIRT). Der er tilføjet en definition af CSIRT, og i bemærkningerne til definitionen fremgår det, at det i Danmark er Center for Cybersikkerhed, der fremover forventes at varetage funktionen som CSIRT.

3. Operatører af væsentlige tjenester

Erhvervsflyvningens Sammenslutning vurderer ikke, at deres medlemmer udpeges som de mest samfundskritiske operatører inden for luftfart.

Danske Rederier, Rederiforeningen og Færge Rederierne vurderer, at relationen til skibsfarten og skibenes interaktion med danske havne ikke vil være at betragte som en væsentlig transporttjeneste i direktivets forstand.



Trafikselskaberne i Danmark påpeger, at der er ikke ubetydelige konsekvenser, herunder administrative og økonomiske byrder, ved at blive udpeget som operatør af væsentlige tjenester, og opfordrer ministeriet til at præcisere yderligere, hvad der lægges vægt på i forbindelse med udpegningen af operatører.

Inden for transportsektoren er der meget forskelligartede operatører, og de kriterier, der ligger til grund for, at en operatør bliver omfattet af reglerne, kan ikke beskrives detaljeret, men vil bero på en konkret vurdering.

Lovforslaget omfatter alene de operatører, der af transport-, bygnings- og boligministeren udpeges som operatører af væsentlige tjenester. Der træffes en forvaltningsmæssig afgørelse herom senest den 9. november 2018, og listen over udpegede operatører ajourføres mindst hvert andet år.

Operatørerne kan være både offentlige eller private enheder under transport-, bygnings- og boligministerens ressort. Transport-, bygnings- og boligministeren vil i forbindelse med udpegningen lægge vægt på, at operatøren leverer en transporttjeneste, der er afhængig af net- og informationssystemer og er væsentlig for opretholdelsen af kritiske samfundsmæssige og økonomiske aktiviteter. Ydermere skal en given hændelse inden for net- og informationssystemerne have væsentlige forstyrrende virkninger for leveringen af transporttjenesten, førend operatøren vil blive betragtet som en operatør af væsentlige tjenester i lovforslagets forstand.

Det vil bero på en konkret vurdering, om en hændelse vil få væsentlige forstyrrende virkninger. Transport-, bygnings- og boligministeren tager herunder hensyn til tværsektorielle forhold som antal af brugere, der er afhængig af tjenesten, afhængighed i andre sektorer, konsekvenser, som hændelser kan have med hensyn til omfang og varighed på samfundsmæssige aktiviteter, den nævnte enheds markedsandel, den geografiske udbredelse, samt enhedens betydning med henblik på at opretholde et tilstrækkeligt tjenesteniveau.

Transport-, bygnings- og boligministeren vil fastsætte nærmere regler i en bekendtgørelse om udpegningen af operatører af væsentlige transporttjenester, herunder de kriterier der skal lægges vægt på ved udpegningen af operatørerne.

Det er ministeriets forventning, at der vil være tale om enkelte private operatører og en eller flere operatører, som er en del af den offentlige sektor, som vil blive udpeget som operatører af væsentlige transporttjenester, og at de alle karakteriseres ved at være særdeles store operatører, der har en dominerende status på hver deres område.

Trafikselskaberne i Danmark anser det endvidere for betænkeligt, at ministerens adgang til at afskære klageadgangen over udpegning som operatør alene er



begrundet i, at afgørelsen om udpegning vil være af udpræget teknisk karakter, som forudsætter betydelig indsigt i området.

Transport-, Bygnings- og Boligministeriet bemærker, at det forudsætter en særlig teknisk og faglig ekspertise inden for transportområdet at vurdere hvilke operatører, der skal udpeges. Trafik-, Bygge- og Boligstyrelsen varetager allerede lignende opgaver på en række områder. En afskæring af klageadgangen over udpegning vil være i overensstemmelse med reglerne på lignende sagsområder varetaget af Trafik-, Bygge- og Boligstyrelsen, hvor en særlig teknisk og faglig ekspertise er påkrævet for at træffe afgørelse. Det bemærkes, at de almindelige forvaltningsretlige regler om partshøring, begrundelse m.v. vil blive iagttaget ved udpegelsen af operatører omfattet af lovforslaget.

Øresundsbro Konsortiet fremfører, at såfremt Øresundsbron udpeges som operatør af en væsentlig transporttjeneste, er det vigtigt, at selve udpegningen samt de krav, der stilles i den forbindelse, er samordnet mellem Danmark og Sverige.

Det er specificeret i bemærkningerne, at transport-, bygnings- og boligministeren forud for en eventuel udpegning af en operatør, der leverer en grænseoverskridende tjenesteydelse, vil indgå i dialog med de medlemslande, hvor tjenesteydelsen leveres. Denne dialog skal hjælpe med at vurdere operatørens kritiske karakter med hensyn til grænseoverskridende konsekvenser.

4. Certificering

DSB anfører, at certificering forudsætter en præcis definition af, hvilke systemer der er omfattet af loven, og som dermed kan blive omfattet af certificeringskrav. **DSB** anfører endvidere, at bemyndigelsen til fastsættelse af krav til certificering bør forelægges de berørte virksomheder i form af udkast til konkrete regler.

Med henvisning til lovforslagets § 4, stk. 3, bemyndiges transport-, bygnings- og boligministeren til at fastsætte nærmere regler om foranstaltningerne til at styre risiciene i net- og informationssystemer. Relevante operatører vil blive inddraget i den videre proces med at fastsætte de nærmere regler.

DSB anfører, at en revisorerklæring, der følger den internationale standard, ISAE 3000 "Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger", med et scope vedr. systemsikkerhed i de af loven omfattede togsystemer kunne være et alternativ til en certificering.

Transport-, Bygnings- og Boligministeriet har noteret sig DSB's forslag til alternativ model. Forslaget om en certificeringsmodel bygger på en nærmere vurdering af to modeller for implementering af lovforslaget:



- *En statslig godkendelsesmodel, hvor Trafik-, Bygge- og Boligstyrelsen efter delegation godkender operatørernes risikostyringsforanstaltninger og fører tilsyn hermed.*
- *En certificeringsmodel, hvor operatørerne bliver pålagt at blive certificeret efter en international anerkendt standard efter eget valg.*

I den statslige godkendelsesmodel udarbejder Trafik-, Bygge- og Boligstyrelsen sikkerhedskrav om foranstaltninger af teknisk og organisatorisk karakter, som pålægges operatøren. Styrelsen skal godkende, at operatøren følger de fastlagte krav, og styrelsen fører løbende tilsyn med, at kravene er overholdt.

En statslig godkendelsesmodel vil ikke rumme den samme fleksibilitet for operatørerne som certificeringsmodellen, hvor det er operatørerne der selv vælger, hvilken standard de vil certificeres efter.

Trafik-, Bygge- og Boligstyrelsen fører i dag ikke tilsyn med IT- og informationssystemer hos operatørerne. Styrelsen råder derfor ikke over de ressourcer og IT-kompetencer, der vurderes nødvendige for at kunne føre et effektivt tilsyn med operatørernes efterlevelse af lovforslaget. Den statslige godkendelsesmodel forudsætter derfor, at styrelsen enten rekrutterer medarbejdere med særlig kompetence til at håndtere meget specialiserede IT-sikkerhedsopgaver eller køber denne kompetence hos eksterne konsulenter.

Trafik-, Bygge- og Boligstyrelsens godkendelses- og tilsynsvirkomhed på transportområdet er i dag i vid udstrækning brugerfinansieret i form af gebyrer eller afgifter. Ved en statslig godkendelsesmodel vil styrelsen skulle opkræve gebyrer fra operatørerne til dækning af udgifterne til såvel sagsbehandlingen i styrelsen som viderefakturering for eventuelle eksterne konsulenter, som det skønnes nødvendigt at inddrage i vurderingen af efterlevelsen af reglerne.

Ved certificeringsmodellen dokumenterer operatørerne efterlevelse af de sikkerhedskrav, som fastsættes i loven ved at lade sig certificere i overensstemmelse med en internationalt anerkendt standard for styring af net- og informationssikkerhed.

Metoden med at basere sig på en international anerkendt standard inden for net- og informationssikkerhed tager udgangspunkt i den enkelte institutions risikoprofil og rummer mulighed for, at der implementeres netop de sikkerhedsforanstaltninger og kontrolprocedurer, der er passende for den enkelte operatør. Dermed sikres det, at de sikkerhedskrav, der stilles til de udpegede operatører, er proportionale, og at operatøren ikke pålægges unødige foranstaltninger, men alene skal gennemføre sikkerhedsforanstaltninger og kon-



trolprocedurer, der står i et passende forhold til den enkelte operatørs tjeneste.

Styrelsens tilsyn vil herefter bestå i løbende at verificere, at den enkelte udpegede operatør opretholder sin certificering. Dertil kommer, at styrelsen vil afholde de nødvendige møder med det certificerende organ. Det vil være det certificerende organ, der med sin certificering af operaøren giver sikkerhed for, at de nødvendige foranstaltninger til at forhindre, forebygge og håndtere hændelser i operatørens udpegede net- og informationssystemer, er på plads.

De akkrediterede certificeringsorganer, der beskæftiger sig med certificering efter en international anerkendt standard, har oparbejdet kompetencer på netop dette område, og vil meget målrettet kunne vejlede de enkelte operatører i forhold til fx scopet for certificeringen, og gennemførelsen af de relevante foranstaltninger. De certificerende organer vil – for at der skal være vished om deres faglige kompetencer på området – af samme grund skulle have den nødvendige akkreditering af et akkrediteringsorgan.

Trafik-, Bygge- og Boligstyrelsen vil ikke på samme måde kunne skaffe den nødvendige ekspertise, hvis reguleringen baseres på en godkendelsesmodel, idet styrelsen ikke som godkendende myndighed har de samme muligheder for at gå i dialog om scope, mulige tiltag mv. som et akkrediteret organ har.

På baggrund heraf vurderer Transport-, Bygnings- og Boligministeriet, at den mest hensigtsmæssige model for implementeringen af lovforslaget vil være at stille krav om certificering efter en international anerkendt standard. Kravene vil blive fastlagt nærmere i en bekendtgørelse.

5. Underretning om hændelser

Danske Havne, Danske Rederier, Færge Rederierne og Rederiforeningen, mener ikke, at implementeringen af NIS-direktivet kræver indførelse af nye indberetnings- eller kontrolforanstaltninger for havne og havnefaciliteter, da der allerede eksisterer obligatoriske sikkerhedsforanstaltninger og rapporteringskrav inden for søfartssektoren, som må betragtes som *lex specialis*.

Regler om indberetning af hændelser inden for søfartssektoren, der mindst svarer til de tilsvarende bestemmelser i NIS-direktivet, som implementeret ved dette lovforslag, vil blive betragtet som *lex specialis*.

DSB anfører i forhold til kravet om, at operatøren ”hurtigst muligt” skal foretage underretning om hændelser, at de specielle bemærkninger til forståelsen af ”hurtigst muligt”, jf. lovforslagets § 5, stk. 1, anerkendes, da formuleringen ”i rette tid” er anvendt i de generelle bemærkninger, hvilket virker mere passende.



Transport-, Bygnings- og Boligministeriet bemærker, at det i lovforslagets beskrivelse af gældende ret er anført, at der på jernbaneanrådet er krav om, at data om ulykker og forløbere til ulykker skal indberettes i rette tid. Denne formulering knytter sig således til beskrivelsen af gældende ret. Underretning om hændelser omfattet af lovforslaget skal ske ”hurtigst muligt”. Det indebærer, at operatøren – dog under hensyn til arbejdet med at minimere konsekvenserne af hændelsen – skal underrette myndighederne, så snart operatøren har de nødvendige oplysninger til at vurdere hændelsens omfang, herunder om der overhovedet er tale om en underretningspligtig hændelse.

Erhvervsflyvningens Sammenslutning anfører, at det vil være hensigtsmæssigt, at der offentliggøres et link eller tilsvarende, som kan benyttes til frivillig underretning om hændelser.

Danske Havne, Danske Rederier, Færge Rederierne, IT-Politisk Forening og Rederiforeningen fremfører, at det er vigtigt, at det med den sektorspecifikke implementering sikres, at de respektive myndigheder koordinerer eventuelle relationer til andre sektorer, således at kravet om underretning af myndighederne ved hændelser ikke fører til krav om dobbeltunderretning og unødige byrder for erhvervslivet.

Det forventes, at der oprettes én fælles digital indgang til indberetning af IT-sikkerhedshændelser på Virk.dk. Formålet er at gøre det lettere for virksomheder og myndigheder at efterleve kravene om lovpligtig indberetning af IT-sikkerhedshændelser. Det vil dermed kun være ét sted, at operatøren skal foretage underretningen, som herefter sendes til både de relevante kompetente myndigheder og CSIRT'en. Det forventes, at den fælles digital indgang på Virk.dk også kan benyttes til frivillig underretning om IT-sikkerhedshændelser.

6. Videregivelse af oplysninger og tavshedspligt

DSB mener, at den særlige tavshedspligt i forslagets § 8 bør udvides til også at omfatte oplysninger opnået i forbindelse med tilsyn.

Lovforslaget er blevet ændret på baggrund af de indkomne høringssvar og indeholder i dets nuværende form ikke nogen bestemmelse om en særlig tavshedspligt.

Dette skyldes for det første, at Forsvarsministeriets lovudkast vedrørende internetudvekslingspunkter regulerer Center for Cybersikkerheds adgang til at offentliggøre hændelser, herunder fra andre sektorer. Det vurderes fra Forsvarsministeriets side ikke hensigtsmæssigt, at Center for Cybersikkerhed pålægges tavshedspligt i den sektorspecifikke regulering.



Dernæst er det Transport, Bygnings- og Boligministeriets vurdering, at man ikke kan pålægge private operatører et strafansvar efter straffelovens § 152-152 e.

Samlet set betyder dette, at tavshedspligten kun vil gælde for en del af de personer der vil få adgang til oplysningerne. Det er derfor Transport, Bygnings- og Boligministeriets vurdering, at tavshedspligten vil risikere at kunne medføre en forkert opfattelse om fortrolighed for de operatører der indberetter, hvorfor ministeriet har besluttet at revidere lovtæksten, så den følger den høringsmodel der fremgår af direktivets artikel 14 stk. 6.

DSB foreslår, at der stilles krav om, at kommunikation omkring fortrolige og sensitive oplysninger krypteres.

Transport-, Bygnings- og Boligministeriet noterer sig forslaget og bemærker, at de nærmere regler for kommunikationsmåden fastsættes på bekendtgørelsesniveau. Det fremgår af bemærkningerne til lovforslaget, at der vil kunne fastsættes regler om, at underretningerne skal være digitale og foregå på en given platform.

Dansk Institut for Menneskerettigheder og **IT-Politisk Forening** anser det for problematisk, at Center for Cybersikkerhed varetager rollen som CSIRT og dermed modtager underretninger om hændelser, da Forsvarets Efterretningstjeneste som udgangspunkt er undtaget fra offentlighedslovens anvendelsesområde og fra centrale dele af forvaltningsloven. Forsvarets Efterretningstjeneste er endvidere generelt undtaget fra den gældende persondatalov og det for nyligt fremsatte forslag til en ny databeskyttelseslov (L 68). Med den forventede etablering af CSIRT som en del af Forsvarets Efterretningstjeneste vil CSIRT derfor være generelt undtaget fra den EU-retlige ramme for databeskyttelse, som NIS-direktivets artikel 2 kræver overholdelse af.

Datatilsynet forudsætter, at persondataloven og regler udstedt i medfør heraf vil blive iagttaget i forbindelse med de behandlinger af personoplysninger, der eventuelt vil ske som følge af lovforslagets bestemmelser. Datatilsynet har endvidere gjort opmærksom på, at databeskyttelsesforordningen får virkning fra 25. maj 2018, og at persondataloven samtidig ophæves.

IT-Politisk Forening udtaler, at der bør fastsættes regler, som begrænser behandlingen af personoplysninger til det strengt nødvendige for at klarlægge omfanget af hændelsen og dens eventuelle grænseoverskridende konsekvenser. Der bør desuden være et eksplicit krav om, at disse personoplysninger skal slettes eller anonymiseres hurtigst muligt.

Transport-, Bygnings- og Boligministeriet har præciseret i bemærkningerne til lovforslaget, at i tilfælde, hvor der er tale om behandling af personhenførbare oplysninger, vil lovgivningen for databeskyttelse, jf. lov nr. 429 af 31.



maj 2000 om behandling af personoplysninger med senere ændringer samt regler udstedt i medfør heraf, finde tilsvarende anvendelse. Reglerne i databeskyttelsesforordningen, jf. forordning (EU) 2016/679 af 27. april 2016, vil finde anvendelse, når disse får virkning den 25. maj 2018.

Side 9/9

Der henvises i øvrigt til bemærkningerne til nærværende lovforslag .

7. Økonomiske konsekvenser

Danske Regioner anmoder under henvisning til høringssvaret fra Trafikskaberne i Danmark om at få lovforslaget i DUT høring, idet lovforslaget kan have betydelige økonomiske konsekvenser for regionerne. Danske Regioner anmoder om en vurdering af de økonomiske konsekvenser for regionerne.

Såfremt trafikskaberne udpeges som operatører af væsentlige transport-tjenester og underlægges krav om certificering, kan det ikke udelukkes, at der vil skulle iværksættes en DUT-høring. En sådan vil i givet fald blive håndteret behørigt.