Danske Havne

Bredgade 23, 2. tv
1260 København K

Telefon 7211 8100

Ref Eva Fiil Nielsen
efn@danskehavne.dk
Dir 61710706

www.danskehavne.dk

Transport-, Bygnings- og Boligministeriet
Frederiksholms Kanal 27 F
1220 København K
Att.: specialkonsulent Gry Høirup

2. Januar 2018

Høringssvar vedr. udkast til forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Med henvisning til høringsbrev af 29. november 2017 vedr. udkast til implementering af direktiv 2016/1148 (NIS-direktivet), har Danske Havne følgende kommentarer.

Helt overordnet kan Danske Havne tilslutte sig bemærkningerne i Danske Rederiers høringssvar af den 22. december 2017 vedr. udkast til lovforslag om sikkerhed i net- og informationssystemer i transportsektoren.

Af høringsbrevet fremgår det, at Regeringen påtænker at implementere NIS-direktivet sektorvist med det formål at varetage sektorspecifikke forhold, for derved at opnå den bedst mulige beskyttelse af net- og informationssystemer og samtidig sikre, at erhvervslivet ikke pålægges unødvendige byrder.

Danske Havne bifalder særligt hensynet om ikke at pålægge erhvervet unødvendige byrder. På havneområdet beder vi derfor om, at man særligt observerer NIS-direktivets præambel pkt. 10, hvoraf det fremgår, at der allerede eksisterer obligatoriske sikkerhedsforanstaltninger indenfor søfartssektoren og herunder bl.a. for havne og havnefaciliteter.

Danske Havne anser derfor ikke at implementering af NIS-direktivet kræver indførsel af nye indberetnings- eller kontrolforanstaltninger for havne.

Med venlig hilsen,

Eva Fiil Nielsen
PA/Policy Advisor

DanskeRederier

Rederiforeningen af 2010

FærgeRederierne

Transport-, Bygnings- og Boligministeriet
Att.: specialkonsulent Gry Høirup
Frederiksholms Kanal 27 F
1220 København K
Sendt via e-mail: grf@trm.dk

Høringssvar vedr. udkast til lovforslag om sikkerhed i net- og informationssystemer i transportsektoren

22. december 2017

Sagsnummer:
EMN-2016-00289

Der henvises til høringsbrev af 29. november 2017 vedr. udkast til lovforslag om sikkerhed i net- og informationssystemer i transportsektoren, journal nummer: 2017-4685.

Vi noterer os, at der med lovforslaget sker en implementering af 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 (NIS-direktivet) for transportsektoren.

Indledningsvis finder vi, at det er vigtigt, at der med den sektorspecifikke implementering sikres at de respektive myndigheder koordinerer evt. relationer til andre sektorer, således at eksempelvis krav til rapportering ikke fører til krav om dobbeltrapportering og unødige byrder for erhvervslivet.

Vi har noteret os, at søfart er nævnt som mulig enheder i NIS-direktivets bilag 2. Det er imidlertid vores vurdering, at relationen til skibsfarten (national færgefart) og skibenes interaktion med danske havne ikke vil være at betragte som en væsentlig transporttjeneste i direktivets forstand. Desuden mener vi, at færgerne og havnene allerede er omfattet af *lex specialis* hvad angår sikring, bl.a. ved Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 af 31. marts 2004 om bedre sikring af skibe og havnefaciliteter, med de dertil hørende rapporteringskrav.

Derfor er der efter vores opfattelse ikke behov for at udpege national færgefart og danske havne som operatører af væsentlige transporttjenester omfattet af direktivet.

Med venlig hilsen

Morten Glamsø
Chefkonsulent

TRM Gry Høirup

Fra: Johan Nielsen <jon@regioner.dk>
Sendt: 5. januar 2018 10:03
Til: TRM Gry Høirup
Cc: TRM Janette Nowak-Zorde; Henrik Severin Hansen; Birgitte Nymark
Emne: Svar på Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren
Vedhæftede filer: signaturbevis.txt

Til Transport-, Bygnings- og Boligministeriet
Att. TRM Gry Høirup <grh@TRM.dk>
Kopi: jbn@trm.dk

Vedr. Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Danske Regioner skal under henvisning til høringssvaret fra TID (Trafikselskaberne i Danmark) anmode om at få ovennævnte lovforslag i DUT høring, idet svaret fra TiD antyder, at lovforslaget kan have betydelige økonomiske konsekvenser for regionerne. Danske Regioner skal samtidig anmode ministeriet om at foretage en vurdering af de økonomiske konsekvenser for regionerne.

Med venlig hilsen

Johan Nielsen
Seniorkonsulent
Center for Vækst, Erhverv og Regional Udvikling
(VERU)

Danske Regioner
Dampfærgevej 22
2100 København Ø

T 35 29 81 74
E jon@regioner.dk

Officiel post bedes sendt til
regioner@regioner.dk

www.regioner.dk

Fra: TRM Gry Høirup [mailto:grh@TRM.dk]
Sendt: 29. november 2017 15:38
Cc: 'christian.algreen.ussing@alstomgroup.com' <christian.algreen.ussing@alstomgroup.com>; 'dacta@dacta.dk' <dacta@dacta.dk>; Dansk Jernbaneforbund <dj@djf.dk>; Post <post@lokaltog.dk>; 'nj@nj.dk' <nj@nj.dk>
Emne: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Til høringsparterne

Hermed sendes forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren.

Udover forslag til ny lov sendes høringsbrev.

Høringsfristen er **tirsdag den 2. januar 2018, kl.10.00.**

Høringssvar til forslag til ny lov kan fremsendes pr. e-mail til trm@trm.dk med kopi til tbj@trm.dk

Bemærkninger og spørgsmål til lovforslaget bedes sendt til grh@trm.dk med kopi til jbn@trm.dk

Link til høringsportalen: https://hoeringsportalen.dk/Hearing/Details/61332

Venlig hilsen

Thea Bang Schou Jensen
Stud.jur

Transport-, Bygnings- og Boligministeriet
Ministry of Transport, Building and Housing
Internationalt Kontor
Frederiksholms Kanal 27 F
DK-1220 København K

Telefon: +45 72 26 71 46
tbj@trm.dk
www.trm.dk

DATATILSYNET

Transport-, Bygnings- og Boligministeriet
Frederiksholms Kanal 27 F
1220 København K

Sendt til: grh@trm.dk og jbn@trm.dk
CC: jm@jm.dk

2. januar 2018

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2017-112-0805
Dok.nr. 457034
Sagsbehandler
Makar Juhl Holst
Direkte 3319 3236

Vedrørende udkast til lovforslag om sikkerhed i net- og informationssystemer i transportsektoren – ministeriets j.nr. 2017-4685

Ved brev af 29. november 2017 har Transport-, Bygnings- og Boligministeriet anmodet om Datatilsynets bemærkninger til ovennævnte udkast til lovforslag.

Datatilsynet forudsætter, at persondataloven[1] og regler udstedt i medfør heraf, herunder sikkerhedsbekendtgørelsen[2], vil blive iagttaget i forbindelse med de behandlinger af personoplysninger, der eventuelt vil ske som følge af lovforslagets bestemmelser.

Udkastet giver ikke umiddelbart Datatilsynet anledning til bemærkninger.

Datatilsynet skal for god ordens skyld gøre opmærksom på, at databeskyttelsesforordningen[3] får virkning fra 25. maj 2018, og at persondataloven samtidig ophæves.

Kopi af dette brev sendes til Justitsministeriets Lovafdeling til orientering.

Med venlig hilsen

Makar Holst

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
[2] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.
[3] 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.

Til: Transportministeriet (trm@trm.dk)
Cc: TRM Thea Bang Schou Jensen (tbj@TRM.dk)
Fra: Aneela.Iqbal@deutschebahn.com (Aneela.Iqbal@deutschebahn.com)
Titel: Vedr. j.nr. 2017-4685 - Vores reference: 2008-12-14
Sendt: 19-12-2017 16:14:29

Att.: Thea Bang Schou Jensen

DB Cargo Scandinavia A/S (herefter DBCSc) skal hermed afgive høringssvar til Transport- og Byggeministeriets høring af 29. november 2017 over forslag til lov om sikkerhed i net- og informationssystemer i transportsektoren.

Høringen giver ikke anledning til bemærkninger fra DBCSc.

Med venlig hilsen/Best regards

Aneela Iqbal
Legal Adviser/Deputy Head of Safety Management
Safety Management

DB Cargo Scandinavia A/S
Spotorno Allé 12
DK-2630 Taastrup

Office +45 88 30 09 29 | Mobile +45 42 14 23 58 | Email aneela.iqbal@deutschebahn.com | Website www.dbcargo.com/dk

Transport-, Bygnings- og Boligministeriet
Frederiksholms Kanal 27 F
1220 København K

Høringssvar vedr. udkast til forslag til lov om sikkerhed i net- og informationssystemer i transportsektoren

DSB

22. december 2017

DSB
Telegade 2,
2630 Taastrup

CVR 25 05 00 53
www.dsb.dk

Transport-, Bygnings- og Boligministeriets har ved mail af 29. november 2017 sendt udkast til forslag til lov om sikkerhed i net- og informationssystemer i transportsektoren i høring.

DSB takker for muligheden for at bidrage med høringssvar og skal allerede indledningsvis anerkende det store arbejde, der er blevet gjort siden præ-høringsrunden. DSB har således noteret sig, at vise af de af DSB under mødet anførte forhold nu er afspejlet i det udkast til forslag, som ministeriet har sendt i høring.

Generelle bemærkninger
DSB anerkender det store arbejde der er blevet gjort med udkastet til lovforslaget for at omsætte direktivteksten til dansk lovgivning.

DSB anser det for positivt, at der i lighed med beredskabsområdet i øvrigt, lægges op til etablering af Nationalt Centralt Kontaktpunkt og ser frem til at modtage nærmere oplysninger om funktion og opgaver.

DSB anser det som særdeles positiv at udkastet til lovforslaget i sin nuværende form bedre afspejler behovet for at sikre fortrolighed og sikring af forretningsfølsom information vedrørende hændelser, jf. fx § 9 og afsnit 2.2.2 i de generelle bemærkninger. DSB er enig i, at det er af afgørende betydning at kunne have en åben og tillidsfuld kommunikation mellem virksomheder og myndigheder i tilfælde af hændelser, herunder at der er opsat de fornødne barrierer i denne kommunikation til, at oplysninger om et evt. hul i virksomhedens net- og informationssystemer ikke kommer til uvedkommendes kundskab. Sådanne informationer vil netop risikere at øge uvedkommendes interesse til at udnytte svagheden i systemerne og dermed forværre en aktuel hændelse, samt forhindre imødegåelsen af hændelsen og minimering af hændelsens konsekvenser.

DSB tillader sig ligeledes generelt at bemærke, at gennemarbejdning af udkastet til lovforslaget efterlader indtrykket, at bestemmelserne, herunder særligt definitionerne, kunne have gavn af at blive mere entydige i deres formulering og dermed blive forståelige og anvendelig uden behov for fortolkning ved hjælp af bemærkningerne til lovforslaget.

Konkrete bemærkninger

Ad § 2, nr. 2) – definitionen af "Sikkerhed i net- og informationssystemer"

DSB anerkender, at ministeriet lægger op til definitioner, der holder sig tæt op ad definitionerne i direktivteksten. Dette giver dog visse usikkerheder i forhold til definitionernes nøjagtighed. Således fremgår det ikke tydeligt, hvad det indebærer, at et Net- og informationssystem har evnen til, på et givet sikkerhedsniveau, at modstå handlinger. Det er således ikke entydigt, hvad der skal forstås under "*et givent sikkerhedsniveau*", det vil sig, hvor bagatelgrænsen lægges og hvordan dette har indflydelse på vurderingen af om et systems vurderes som værende sikker.

En skarpere afgrænsning af definitionen kan bidrage til forståelsen af, hvilke systemer der anses for værende omfattet af loven – det vil sige at det alene er konkrete systemer, der bidrager til konkret leverance af en transportydelse, således at det ikke kan misforstås til at omfatte eksempelvis windows programmer, men alene relevante systemer, eksempelvis disponeringssystemer, som er definereret af jernbanevirksomheden, se også bemærkningerne nedenfor vedrørende §§ 3 og 4.

Ad § 2, nr. 3, litra a) – definitionen af "Net- og informationssystemer"

Der er tale om en særdeles bred definition af net og informationssystemer, der stort set omfatter alle digitale systemer i en jernbanevirksomhed, ikke blot systemerne, der er af afgørende betydning for leverance af den væsentlige transportydelse. DSB anerkender, at definitionen bygger på selve direktivteksten, som i sin natur vil være en kompromistekst og dermed bredt favnende under hensyntagen til medlemslandenes forskellige tekniske forudsætninger og systemer.

Idet lovforslaget dækker hele transportsektoren, ville det være at foretrække med sektorspecifikke definitioner, der for operatørerne ville gøre det nemmere at forstå scope for lovforslaget og afgræsning ift. systemer omfattet af lovforslaget. DSB har noteret sig, at definitionen, sammen med de underliggende litra til nummer 3, ville komme til at omfatte ethvert element (enhed eller program), selv et redskab som fx en trådløs mus.

Ad § 2, nr. 3, litra c) - definitionen af "Net- og informationssystemer"

Under litra c er der tale om "data", det vil sige informationer indeholdt i systemer, uden dog at dette på nogen måde definerer, hvad der udgør et system. Litra c) synes på den baggrund misvisende uden en definition af, hvad der forstås ved et system.

Ad § 2, nr. 3, litra b)

DSB tillader sig at gøre opmærksom på, at brugen af et "program" til udførelse af automatisk behandling af data, som anført i netop denne definition, medfører at begrebet på en formentlig utilsigtet måde kommer til at omfatte mere end de ellers i udkastet til lovforslaget omtalte systemer.

Ad § 2, nr. 4, inkl. bemærkninger – definitionen af en "risiko"

Begreber som risiko, farer og barrierer er veletablerede og definerede begreber i den jernbanesikkerhedsmæssige begrebsverden, relateret til den risikoprofil en

jernbanevirksomhed lovgivningsmæssig er forpligtet til at etablere og drifte. Definitionen af en risiko, som den står i udkastet til forslaget, er rettelig en definition af en fare. En fare er enhver rimelig omstændighed, der kan indtræffe, imens en risiko er den sandsynlighed, som faren vil indtræffe med. DSB foreslår på den baggrund at enten definitionen omdøbes til "fare", eller at der laves en definition af, hvad der forstås ved "risikoen". Af hensyn til en fælles forståelse ville det være at foretrække, at der var definition af begge begreber, såvel "fare", som også "risiko".

I forhold til bemærkningen til § 2, stk. 4), er der anført, at risici skal styres ved systematisk anvendelse af ledelsespolitikker, procedurer og praksis, uden dog at det på nogen måde fremgår, hvad der eksempelvis skal forstås ved en "ledelsespolitik" endsige, at der er stillet krav om en sådan i udkastet. DSB er på den baggrund i tvivl om, hvilke administrative konsekvenserne oplysningerne i dette afsnit af de specifikke bemærkninger indebærer.

Ad § 2, nr. 5 – definitionen af en hændelse

Der er tale om en særdeles bred definition af en "hændelse" der, taget definitionen for pålydende, kunne omfatte kortvarige strømafbrydelser eller programfejl i systemet. DSB ville foretrække at definitionen bedre afspejlede art og omfang en hændelse skal have for at være omfattet af loven, også henset til tydeligheden af lovteksten, således at denne kan stå uden behov for tolkning ved hjælp af de informationer, der fremgår af de specifikke bemærkninger til bestemmelsen.

Herudover omtales i definitionen også hændelsens effekt, som "egentlig" negativ og som en "indvirkning". Det fremgår desværre på ingen måde, hvad der skal forstås ved en indvirkning, hvilket kan forstås som påvirkning uden konsekvens. En mere hensigtsmæssig definition af effekten kunne være en *afgørende negativ konsekvens*, også henset til den særdeles brede beskrivelse af hændelsens konsekvenser i udkastet til § 5, stk. 2. Sammenlignelig er der på jernbanesikkerhedsområdet en kvalificering og differentiering af hændelsestyper efter væsentligheds- og alvorlighedsgrad, der gør det nemmere i forhold til både håndtering af hændelser og kommunikation herom til og fra myndighederne.

Ad §3 og § 4 – omfattede systemer

Det fremgår desværre ikke tydeligt af §'en, at udkast til lovforslaget alene omfatter de net- og informationssystemer, der er af afgørende betydning for leverance af den væsentlige transporttjeneste, det vil sige, at forslaget ikke omfatter fx Outlook eller Excel, men eksempelvis disponeringssystemer.

Umiddelbart fremgår dette alene tydeligt af § 4, stk. 1, 1. led. DSB tillader sig at foreslå, at det under § 2, nr. 3) præciseres, at de systemer, der er omfattet alene vedrører net- og informationssystemer, som virksomhederne anvender til den del af deres aktiviteter, hvor en hændelse vil få væsentlig forstyrrende virkning for leveringen af den nævnte transporttjeneste, sådan som det også fremgår af de specifikke bemærkninger til bestemmelsen, side 17, andet afsnit.

Ad § 4 – forholdsmæssighed i imødegåelse af risici
Det fremgår af bestemmelsens stk. 1, 1. pkt., at virksomheden skal træffe "passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risici". DSB tillader sig, under henvisning til § 4, stk. 3, samt de generelle bemærkninger, afsnit 2.1.3, udkastets side 9, 3. afsnittet gå ud fra at der ved fastsættelse af regler til håndtering af barrierer vil blive tale om at det er virksomhederne, der umiddelbart afgør barrierernes tilstrækkelighed, under hensyntagen til at de skal passe til og ikke utilsigtet forstyrre virksomhedens almindelige drift i øvrigt, således som det også fremgår af de specifikke bemærkninger til bestemmelsen, på side 17, 3. afsnit.

Ad § 4, stk. 3 – certificering
DSB har noteret sig, at der i medfør af lovforslaget vil kunne udstedes regler om, at der skal ske akkrediteret certificering af net- og informationssystemerne, uden dog at det nærmere fremgår, hvad dette kan indebære. DSB har noteret sig bemærkningerne til bestemmelsen, men har på det foreliggende grundlag svært ved at vurdere omfanget af en eventuel certificeringsordning. DSB tillader sig på den baggrund at bemærke, at en certificering for det første forudsætter en præcis definition af, hvilke systemer, der er omfattet af loven og som dermed kan blive omfattet af certificeringskrav, se også hertil "*Ad § 2, nr. 3, litra a) og c)* ".

DSB bliver hvert år revideret af flere revisionsinstanser, herunder Rigsrevisionen, Ekstern og intern Revision. Endvidere modtager DSB både generelle og specifikke revisorerklæringer fra DSB's outsourcing leverandør. En revisorerklæring, der følger den internationale standard, ISAE 3000 "Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger", kunne med et scope vedr. systemsikkerheden i de af loven omfattede togsystemer være et alternativ til en certificering.

Ad § 7 – kommunikationsmåden
Da der i udkast til § 7, lægges op til at kommunikationen mellem det Nationale Centrale Kontaktpunkt og operatørerne skal være digital, finder DSB det hensigtsmæssigt, at der samtidig etableres tydelige regler for ikke blot den i stk. 1, omtalte form og indhold, men også kommunikationsmåden. Baggrunden er en interesse i at denne kommunikation kan ske så åben som mulig og siden der vil være tale om kommunikation af fortrolig og sensitive oplysninger, tillader DSB sig at foreslå krav om kryptering af denne kommunikation.

Ad § 8 – udbredelse af oplysninger om hændelser
Idet der i tilfælde af hændelser vil være tale om særdeles forretningsfølsomme oplysninger foreslår DSB, at det tilføjes bestemmelsen, at orienteringen sker i dialog med den eller de berørte virksomhed(er) og under hensyntagen til den fornødne informationssikkerhed i formidlingen af informationerne om hændelsen. Dette for at forhindre, at denne kommunikation risikerer at blive hacket og dermed afsløre en mulig svaghed i en virksomheds systemer for uvedkommende.

DSB tillader sig i den forbindelse at bemærke, at fortroligheden er særlig vigtig i den indledende fase af en eventuel erkendt sårbarhed/kompromittering, da der typisk i denne fase endnu ikke er etableret kompenserende og mitigerende foranstaltninger og sårbarheden som potentielt fortsat vil kunne udnyttes.

Ad § 9 - tavshedspligten
Der lader til at være en uoverensstemmelse mellem hensynet i stk. 1 og formuleringen i stk. 1 "jf. dog stk. 2 og 3". Hensynet med stk. 1 er at pålægge strafbelagt tavshedspligt. Hensynet med stk. 2 er en modifikation hertil, der giver ministeren mulighed for at kommuniker i et vist omfang om en hændelse med andre end virksomheden.

Hensynet i stk. 3 er at sikre, at denne kommunikation i stk. 2 ikke kommer til at omfatte 4 konkret opremsende særligt følsomme områder, det vil sige her sker der igen en indskrænkning af åbenheden, hvilket er i overensstemmelse med hensynet i stk. 1. På den baggrund kan henvisningen "jf. dog", i stk. 1, alene vedrøre stk. 2, idet stk. 3 er en modifikation til stk. 2, der skal sikre og opretholde tavshedspligten i overensstemmelse med intentionen og hensynet i stk. 1.

Formuleringen i stk. 1 bør på den baggrund rettelig alene være "jf. dog stk. 2".

Ad § 10, stk. 1 – informationssikkerhed i forbindelse med tilsyn
Idet det af § 9 fremgår, at denne særlige tavshedspligt alene gælder hændelser, foreslår DSB at tavshedspligten udvides til også at omfatte oplysninger opnået i forbindelse med tilsyn. Baggrunden herfor er, at ministeriet, jf. § 10, stk. 1, 2. pkt., kan anmode om at virksomheden afgiver de oplysninger, som ministeriet anser for værende nødvendige. Idet et tilsyn er udtryk for indgående fokus på et eller flere konkrete områder, vil der i forbindelse med tilsyn kunne fremkomme særdeles forretningsfølsomme oplysninger, der i uvedkommendes kendskab kan medføre en hændelse. Dette kan ikke være hensigten med et tilsyn, hvorfor DSB foreslår, at kommunikationen i forbindelse med et tilsyn omfattes af de samme beskyttelseshensyn, som kommunikationen i forbindelse med en hændelse.

Ad § 12, stk. 1, nr. 1) – håndteringen af "hurtigst muligt"
DSB tillader sig at gå ud fra, at myndighederne i forhold til vurderingen af om underretning er sket "hurtigst muligt", tager højde for, at de personer, der vil kunne foretage den fornøden underretning og ligge inde med de relevante informationer vil være de samme personer, der vil være beskæftiget med at begrænse konsekvenserne af en hændelse. Dette særligt henset til at formuleringen, der benyttes i de generelle bemærkninger, afsnit 2.3.1., side 11, sidste afsnit er "i rette tid", hvilket virker mere passende. DSB anerkender på den baggrund også de specifikke bemærkninger hertil på s. 18, i relation til § 5, stk. 1.

Ad de generelle bemærkninger afsnit 3.1 – certificeringen
DSB tillader sig at kommentere afsnit 3.1, selv om der er tale om konsekvenser for det offentlige, idet afsnittet indeholder oplysninger vedrørende certificering og

forventninger til de omfattede virksomheder. I udkastet til forslagets § 4, stk. 3, sidste pkt., omtales der kort akkrediteret certificering, uden dog at der af lovforslaget i øvrigt fremgår, hvad denne certificering vil komme til at indebær. Det er på den baggrund vanskeligt for DSB, på grundlag af det foreliggende udkast til forslag, at vurdere omfanget af de økonomiske og driftsmæssige konsekvenser af en certificeringsordning. Det er således ikke muligt for DSB for nuværende at vurdere om de under afsnit 3.2. anslåede udgifter for certificering på op til 200.000 kr. i engangsomkostninger og 40.000-100.0000 kr. i årlige vedligeholdelsesomkostninger er korrekt anslået.

DSB anser det endvidere for uhensigtsmæssigt, at oplysninger omkring certificeringen i vidt omfang alene er at finde i bemærkningerne til § 4, og ser på den baggrund frem til, at bemyndigelsen til fastsættelse af krav til certificeringen forelægges berørte virksomheder i form af udkast til konkrete regler. DSB deltager gerne i eventuel fornøden dialog om eksisterende ordning angående revision og godkendelse af DSB's systemer.

Afsluttende bemærkninger

DSB står selvfølgelig til rådighed for uddybning og forklaring af ovenstående bemærkninger, samt de oplysninger, som Transport-, Bygnings, og Boligministeriet skulle anse for fornødne for at kunne vurdere ovenstående. DSB værdsætter den åbne og konstruktive dialog, der har været om det nu foreliggende udkast til lovforslag og bidrager gerne i dialog om den videre udvikling af området og reguleringen med viden og erfaringer.

TRM Gry Høirup

Fra: ES-DAA <es@es-daa.dk>
Sendt: 29. december 2017 10:42
Til: Mail TRM; TRM Gry Høirup
Cc: TRM Thea Bang Schou Jensen; TRM Janette Nowak-Zorde; ES-DAA
Emne: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren: ES 306-17

ES 306-17

Erhvervsflyvningens Sammenslutning (ES) takker for muligheden for at deltage i denne høring om forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren.
ES vurderer ikke, at ES medlemmer udpeges som de mest samfundskritiske operatører indenfor luftfart. Det noteres imidlertid, at der i kapitel 4 "Underretning og videregivelse af oplysninger" anføres, at transporttjenester på frivillig basis kan foretage underretning om en hændelse, som vil kunne få væsentlige forstyrrende virkninger for leveringen af den nævnte transporttjeneste. Til en sådan frivillig indberetning vil det være hensigtsmæssigt, at der findes et bekendtgjort link eller tilsvarende, hvor man kan foretage denne indberetning.
ES har ikke yderligere bemærkninger.

Med venlig hilsen / Best Regards
Dan Banja
Oberstløjtnant / Lt. Colonel
Generalsekretær / Secretary-General
Vice chair ECOGAS & Member of EASA GA.COM
Blålersvej 51
DK-2990 Nivå
Mobil: +45 2480 2256
www.es-daa.dk

INSTITUT FOR
MENNESKE
RETTIGHEDER

Transport-, Bygnings- og Boligministeriet
Frederiksholms Kanal 27 F
1220 København K
Danmark

Att. Specialkonsulent Gry Høirup, grh@trm.dk
Kopi til jbn@trm.dk

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
MOBIL 9132 5775
LGH@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 17/02666-2

4. JANUAR 2018

HØRING OVER UDKAST TIL LOVFORSLAG OM SIKKERHED I NET- OG INFORMATIONSSYSTEMER I TRANSPORTSEKTOREN (NIS-DIREKTIVET)

Institut for Menneskerettigheder er blevet opmærksom på, at Transport-, Bygnings- og Boligministeriet har sendt et udkast til et lovforslag om sikkerhed i net- og informationssystemer i transportsektoren i høring.

Udkastet til lovforslag er et af flere forslag, der gennemfører det såkaldte NIS-direktiv (direktiv 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen). Udkastet gennemfører således direktivet på Transport-, Bygnings- og Boligministeriets område, samtidig med at andre udkast til lovforslag er udarbejdet på andre ministerområder.

Instituttet har en bemærkning vedrørende videregivelse af oplysninger til det nationale centrale kontaktpunkt (udkastets kapitel 4).

Det nationale kontaktpunkt i Danmark – en såkaldt "CSIRT" (Computer Security Incident Response Team – forventes at blive Center for Cybersikkerhed, som er en del af Forsvarets Efterretningstjeneste, så vidt instituttet forstår via et udkast til lovforslag, der skal gennemføre NIS-direktivet på Forsvarsministeriets område.

CSIRT'en skal efter direktivet blandt andet monitorere og håndtere IT-sikkerhedshændelser på nationalt plan, iværksætte tidlig varsling om risici og hændelser og deltage i et CSIRT-netværk i EU.

I 2014, da lovforslaget til lov om Center for Cybersikkerhed (lov nr. 713 af 25. juni 2014) var i høring, bemærkede instituttet det problematiske i, at en række nationale IT-sikkerhedsopgaver, som hidtil havde ligget i civilt regi, blev forankret i Forsvarets Efterretningstjeneste. Forsvarets Efterretningstjeneste er som udgangspunkt undtaget fra offentlighedslovens og persondatalovens anvendelsesområde og fra

centrale dele af forvaltningsloven (aktindsigt, partshøring, begrundelse).

Med nærværende udkast til lovforslag fastsættes, at offentlige og private operatører af væsentlige transporttjenester, herunder inden for lufttransport, jernbanetransport, søfart og vejtransport, hurtigst muligt skal underrette blandt andet det nationale centrale kontaktpunkt om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige transporttjenester, som de leverer (§ 5).

En hændelse er en negativ indvirkning på sikkerheden i de net- og informationssystemer, der er af afgørende betydning for leveringen af den væsentlige transporttjeneste (§ 2, nr. 5).

For alle operatører af transporttjenester er der endvidere adgang til på frivillig basis at underrette ministeren om hændelser, der har væsentlige konsekvenser for udøvelsen af transporttjenesterne (§ 6, jf. § 1, stk. 2). Ifølge bemærkningerne til § 6 kan frivillig underretning dog også ske til det nationale kontaktpunkt, så der ser ud til at være en inkonsistens i formuleringen af selve bestemmelsen og bemærkningerne.

Det nationale kontaktpunkt kan, i det omfang det er nødvendigt for dets funktion, videreformidle oplysninger om hændelser til nationale kontaktpunkter i andre medlemsstater (§ 8).

I takt med at NIS-direktivet bliver gennemført i lovgivning vedrørende en række samfundssektorer, herunder transportsektoren med dette udkast, vil stadig flere oplysninger blive udvekslet med det nationale kontaktpunkt, forventeligt i Forsvarets Efterretningstjeneste.

Instituttet har ikke indsigt i, i hvilket omfang de relevante net- og informationssystemer i transportsektoren behandler personoplysninger. I det omfang, der behandles personoplysninger, følger det af NIS-direktivets artikel 2, stk. 1, at behandling af personoplysninger i henhold til direktivet sker i overensstemmelse med EU's databeskyttelsesdirektiv. Fra 25. maj 2018 vil det i stedet være EU’s databeskyttelsesforordning, der finder anvendelse.

Forsvarets Efterretningstjeneste er imidlertid som nævnt generelt undtaget fra den gældende persondatalov og det for nyligt fremsatte forslag til en ny databeskyttelseslov (L 68). De gængse regler for databeskyttelse gælder således ikke for Forsvarets Efterretningstjeneste.

Med den forventede etablering af det nationale kontaktpunkt som en del af Forsvarets Efterretningstjeneste, vil det nationale kontaktpunkt derfor være generelt undtaget fra den EU-retlige ramme for databeskyttelse, som NIS-direktivets artikel 2 kræver overholdelse af.

Lovudkastet bør redegøre for disse forhold, herunder for hvordan udkastet forholder sig til reglerne for databeskyttelse.

- Institut for Menneskerettigheder anbefaler, at ministeriet præciserer i lovforslaget, hvorledes beskyttelsen af personoplysninger i den danske gennemførelse af NIS-direktivet kan leve op til kravet i direktivets artikel 2 (samt artikel 8 i EU's charter om grundlæggende rettigheder).

Instituttet ønsker i den forbindelse endnu en gang at fremhæve det principielt problematiske i, at centrale, civile samfundsstrukturer i Danmark skal varetages af Forsvarets Efterretningstjeneste med de begrænsninger, det giver i forhold til indsigt og databeskyttelseskrav. Instituttet kan i den forbindelse henvise til sit høringssvar af 4. marts 2014 til lovforslaget til lov om Center for Cybersikkerhed, der vedlægges.

Der henvises til ministeriets sagsnr. 2017-4685.

Med venlig hilsen

Lise Garkier Hendriksen
CHEFKONSULENT

Transport-, Bygnings- og Boligministeriet
Frederiksholms Kanal 27 F
1220 København K

Sendt per email til **grh@trm.dk** med
kopi til **jbn@trm.dk**

IT-Politisk Forening
c/o Jesper Lund
Carl Bernhards Vej 15, 2.tv
1817 Frederiksberg C

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 1. januar 2018

Høringssvar vedr. udkast til lovforslag om sikkerhed i net- og informationssystemer i transportsektoren

Regeringen har valgt at gennemføre NIS-direktivet med sektorspecifikke love, hvor en eksisterende institution under det pågældende ministerium får tilsynsopgaven som kompetent myndighed.

NIS-direktivets artikel 8, stk. 1 overlader det til medlemsstaterne at fastsætte, om der skal være en eller flere kompetente myndigheder. En kompetent myndighed for hvert ministeriums område er som sådan inden for rammerne af artikel 8, stk. 1. Hvis der kommer 4-5 kompetente myndigheder i Danmark (jf. sektoropdelingen i bilag II i NIS-direktivet), kan tilsynsressourcerne blive spredt mere end godt er, og synergieffekter mellem forskellige tilsynsområder kan blive vanskelige at udnytte.

Et væsentligt element i NIS-direktivet er at medlemsstaterne skal vedtage en samlet national strategi for sikkerheden i net- og informationssystemer, og der skal være en effektiv informationsudveksling på tværs af sektorer på nationalt plan samt mellem EU-landene på internationalt plan. De tværgående opgaver vil blive varetaget af de(n) danske CSIRT-enhed(er) og det centrale kontaktpunkt, jf. NIS-direktivet. Ansvaret for disse funktioner er ikke omtalt i lovforslagets bemærkninger, men ifølge de øvrige lovudkast om gennemførelse af NIS-direktivet (fra Sundheds- og Ældreministeriet, Erhvervsministeriet og Forsvarsministeriet) er det regeringens hensigt, at Center for Cybersikkerhed skal

udføre opgaverne som CSIRT og centralt kontaktpunkt.

Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, som generelt opererer under andre rammebetingelser end civile myndigheder, for eksempel med betydelige undtagelser fra offentlighedsloven, forvaltningsloven og persondataloven. IT-Politisk Foreninger finder det meget betænkeligt, at Center for Cybersikkerhed via gennemførelsen af NIS-direktivet får en så betydelig rolle i forhold til cybersikkerheden i den offentlige og private sektor i Danmark. Af principielle årsager mener vi, at de(n) danske CSIRT(er) og det centrale kontaktpunkt bør være civile myndigheder.

Det gælder ikke mindst i de situationer, hvor det kan blive nødvendigt at behandle personoplysninger i forbindelse med underretning af den kompetente myndighed om hændelser, jf. NIS-direktivets artikel 14, stk. 3. Dette punkt uddybes nedenfor.

Behandling af personoplysninger i forbindelse med underretning om hændelser

Lovforlagets § 5, stk. 1, jf. NIS-direktivets artikel 14, stk. 3, fastsætter en pligt til hurtigst muligt at underrette den kompetente myndighed (Transport-, Bygnings- og Boligministeriet) og det Nationale Centrale Kontaktpunkt om hændelser, der har væsentlig betydning for kontinuiteten af de leverede tjenester. Efter regeringens overordnede plan for gennemførelse af NIS-direktivet vil det Nationale Centrale Kontaktpunkt være en institution under Forsvarets Efterretningstjeneste (Center for Cybersikkerhed).

NIS-direktivets artikel 14, stk. 3 kræver underretning af enten den kompetente myndighed eller en CSIRT enhed (der i den danske gennemførelse af NIS-direktivet vil være sammenfaldende med det Nationale Centrale Kontaktpunkt). Lovforslagets § 5, stk. 1 fastsætter således en underretningspligt over for to forskellige offentlige myndigheder, hvilket kan være mere administrativt byrdefyldt for de udpegede operatører af væsentlige transporttjenester.

I nogle tilfælde vil de nødvendige oplysninger i forbindelse

med underretningen om en hændelse indeholde personoplysninger. Det kunne være IP-adresser, men også oplysninger fra et IT-systems databaser, som er forsøgt hacket (exfiltreret) og måske optræder i logfiler. Dette spørgsmål omtales ikke i lovforslagets bemærkninger. Efter IT-Politisk Forenings opfattelse bør der fastsættes lovregler (eventuelt i bekendtgørelsesform), 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.

NIS-direktivets artikel 2, stk. 1 kræver, at behandling af personoplysninger i henhold til direktivet sker i overensstemmelse med direktiv 95/46/EF, og fra 25. maj 2018 databeskyttelsesforordningen (EU) 2016/679. Ifølge den nuværende persondatalov, og det forslag til ny databeskyttelseslov som Justitsministeren har fremsat 25. oktober 2017 (L 68), er Forsvarets Efterretningstjeneste (FE) undtaget fra de EU-retlige regler om databeskyttelse. Undtagelsen er for FE som institution, og vil derfor også gælde, når FE udøver aktiviteter inden for EU-retten, eksempelvis cybersikkerhedsopgaver i forbindelse med NIS-direktivet.

Hvis den fuldstændige undtagelse fra databeskyttelses-forordningen opretholdes for Center for Cybersikkerhed (under FE), vil det efter IT-Politisk Forenings opfattelse ikke være muligt at gennemføre NIS-direktivet på en korrekt måde. Beskyttelsen af personoplysninger i den danske gennemførelse af direktivet vil ikke kunne leve op til kravet i NIS-direktivets artikel 2 (samt artikel 8 i Charter om Grundlæggende Rettigheder).

TRM Gry Høirup

Fra: Hoeringer <Hoeringer@naviair.dk>
Sendt: 2. januar 2018 15:14
Til: TRM Gry Høirup
Cc: TRM Janette Nowak-Zorde
Emne: VS: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren
Vedhæftede filer: Høringsbrev NIS.pdf; NIS udkast til lovforslag.pdf; Høringsliste NIS.pdf; signaturbevis.txt; signaturbevis.txt

Til rette vedkommende
Naviair skal hermed takke for høringen og konstatere, at vi ikke har bemærkninger til lovforslaget.

De bedste hilsner, Mona

Fra: Naviair Naviair
Sendt: 29. november 2017 14:37
Til: Hoeringer <Hoeringer@naviair.dk>
Emne: VS: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

---

Fra: TRM Thea Bang Schou Jensen [mailto:tbj@TRM.dk]
Sendt: 29. november 2017 14:20
Emne: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Til høringsparterne

Hermed sendes forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren.

Udover forslag til ny lov sendes høringsbrev.

Høringsfristen er **tirsdag den 2. januar 2018, kl.10.00.**

Høringssvar til forslag til ny lov kan fremsendes pr. e-mail til trm@trm.dk med kopi til tbj@trm.dk

Bemærkninger og spørgsmål til lovforslaget bedes sendt til grh@trm.dk med kopi til jbn@trm.dk

Link til høringsportalen: https://hoeringsportalen.dk/Hearing/Details/61332

Venlig hilsen

Thea Bang Schou Jensen
Stud.jur

Transport-, Bygnings- og Boligministeriet
Ministry of Transport, Building and Housing
Internationalt Kontor
Frederiksholms Kanal 27 F
DK-1220 København K

Telefon: +45 72 26 71 46
tbj@trm.dk
www.trm.dk

RIGSREVISIONEN

Transport-, Bygnings- og Boligministeriet
Gry Høirup
Frederiksholms Kanal 27 F
1220 København K

Landgreven 4
1301 København K

Tlf. 33 92 84 00

rr@rigsrevisionen.dk
www.rigsrevisionen.dk

21. december 2017

6. kontor

J.nr.: 44317

Høring af forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Transport-, Bygnings- og Boligministeriet har den 29. november 2017 sendt forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren i høring.

Rigsrevisionen har udelukkende gennemgået lovforslaget med henblik på statslige revisions- og regnskabsforhold.

Lovforslaget indeholder ikke bestemmelser om statslige regnskabs- eller revisionsforhold. Rigsrevisionen har derfor ingen bemærkninger.

Med venlig hilsen

Mads Mølgaard Nielsen
Fuldmægtig

Til: Transportministeriet (trm@trm.dk)
Cc: TRM Thea Bang Schou Jensen (tbj@TRM.dk)
Fra: mba@moviatrafik.dk (mba@moviatrafik.dk)
Titel: Høringssvar vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren - Trafikselskaberne i Danmark
Sendt: 02-01-2018 09:23:41
Bilag: signaturbevis.txt;

Trafikselskaberne i Danmark har sendt høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren (NIS-direktivet) til medlemmerne, og nedenfor følger bemærkninger:

Movias administration har følgende bemærkninger til det fremsendte lovforslag:

1. Jf. lovforslaget udpeger ministeriet de virksomheder, som er operatør af væsentlige tjenester, og som derfor omfattes af loven. Dette gøres på baggrund af en vurdering, hvor der lægges vægt på, at enheden leverer en transporttjeneste, der er væsentlig for opretholdelse af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af den væsentlige transporttjeneste afhænger af net- og informationssystemer, og at en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den nævnte transporttjeneste.

   Ministeriet anfører i de almindelige bemærkninger, at der har været to mulige fremgangsmåder i spil til denne identificering. I den ene fremgangsmåde er forudsat, at der kan opstilles en række entydige objektive kriterier, som fastslår, hvad der kræves for at ministeriet betragter den pågældende virksomhed som en operatør af væsentlig transporttjeneste. I den anden fremgangsmåde omfattes virksomheden af loven på baggrund af en forvaltningsmæssig afgørelse herom.

   Da det er forbundet med usikkerhed og ikke ubetydelige konsekvenser herunder administrative og økonomiske byrder i form af årlige omkostninger til akkrediteret certificering for den enkelte virksomhed at blive udpeget som operatør af væsentlige transporttjenester, bør det i højere grad, end det er tilfældet med det foreliggende lovforslag, være muligt for virksomheden på forhånd at vurdere risikoen for, om den vil blive omfattet af loven eller ej. Movia anerkender, at der, som ministeriet anfører i de almindelige bemærkninger, kan være udfordringer ved at definere samtlige kriterier for, hvornår en virksomhed omfattes af lovgivningen. Movia opfordrer derfor ministeriet til at præcisere yderligere, hvad der lægges vægt på i forbindelse med udpegningen, jf. lovforslagets § 3, stk. 2.

2. Forslagets § 11, stk. 3 giver ministeren mulighed for at afskære adgangen til at klage over afgørelser, dvs. også afgørelsen over at være blevet udpeget som operatør, § 3, stk. 2.

   I betragtning af at ministeren administrativt kan pålægge udpegede virksomheder engangsomkostninger op til 200.000 kr. og 40-100.000 kr. i årlige vedligeholdelsesomkostninger til certificering vedr. sikkerheden i net- og informationssystemer (beløbene vil være større, såfremt virksomhederne ikke er certificeringsparate), jf. § 4, stk. 3, finder Movia det betænkeligt, at det alene er begrundet i, at afgørelserne vil være af udpræget teknisk karakter, som forudsætter betydelig indsigt i området, jf. Bemærkninger til lovforslagets enkelte bestemmelser.

Med venlig hilsen

Morten Brønnum Andersen

Seniorkonsulent
Trafikselskaberne i Danmark

Mobil: 2320 6131
Mail: mba@moviatrafik.dk

TRAFIKSELSKABERNE

Fra: TRM Gry Høirup [mailto:grh@TRM.dk]
Sendt: 29. november 2017 15:38
Cc: 'christian.algreen.ussing@alstomgroup.com' <christian.algreen.ussing@alstomgroup.com>; 'dacta@dacta.dk'

<dacta@dacta.dk>; Dansk Jernbaneforbund <dj@djf.dk>; Post <post@lokaltog.dk>; 'nj@nj.dk' <nj@nj.dk>
Emne: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Til høringsparterne

Hermed sendes forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren.

Udover forslag til ny lov sendes høringsbrev.

Høringsfristen er **tirsdag den 2. januar 2018, kl.10.00.**

Høringssvar til forslag til ny lov kan fremsendes pr. e-mail til trm@trm.dk med kopi til tbj@trm.dk

Bemærkninger og spørgsmål til lovforslaget bedes sendt til grh@trm.dk med kopi til jbn@trm.dk

Link til høringsportalen: https://hoeringsportalen.dk/Hearing/Details/61332

Venlig hilsen

Thea Bang Schou Jensen
Stud.jur

Transport-, Bygnings- og Boligministeriet
Ministry of Transport, Building and Housing
Internationalt Kontor
Frederiksholms Kanal 27 F
DK-1220 København K

Telefon: +45 72 26 71 46
tbj@trm.dk
www.trm.dk

Til: Transportministeriet (trm@trm.dk)
Cc: Kristina Jæger (krj@oresundsbron.com), Bodil Rosengren (BRO@oresundsbron.com), Bengt Hergart (BHT@oresundsbron.com), Martin Karlsson (mka@oresundsbron.com), Hafez Azzam (HAZ@oresundsbron.com), 'Rolf Sundqvist' (rsu@oresundsbron.com), TRM Thea Bang Schou Jensen (tbj@TRM.dk)
Fra: Ulla V. Eilersen (uve@oresundsbron.com)
Titel: RE: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren
Sendt: 28-12-2017 13:05:07

Øresundsbro Konsortiet (ØSB) har, via S&B, modtaget høringsmateriale vedr. forslag til Lov om sikkerhed i net- og informationssystemer.

Vi har følgende kommentarer:

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, således at:

- Rapportering til respektive lands myndigheder kan ske med én og samme rapport
- ØSB ikke pålægges dobbelte omkostninger til certificering m.m.

Venlig hilsen / Vänliga hälsningar

Ulla V. Eilersen
Sikkerheds- og miljøchef / Safety Manager

Øresundsbron

Vester Søgade 10
DK-1601 København V
Tel.: +45 33 41 60 00 / +46 (0)40-676 60 00
Direct: +45 33 41 6418 / +46 (0)40-676 6418
Mobile: +4520488525
Email: uve@oresundsbron.com

From: Kristina Jæger
Sent: 30. november 2017 13:13
To: Ulla V. Eilersen <uve@oresundsbron.com>
Subject: FW: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Hej Ulla,
Er dette noget, du vil se på og vurdere, om vi har bemærkninger ?

Best Regards

Kristina Jæger
General Counsel / Chefjurist

Øresundsbron

Vester Søgade 10
DK-1601 København V
Tel.: +45 33 41 60 00 / +46 (0)40-676 60 00
Direct: +45 33 41 6413 / +46 (0)40-676 6413
Mobile: +4560650555
Email: krj@oresundsbron.com

From: Louise Friis [mailto:lfi@SBF.DK]
Sent: 30. november 2017 08:57
To: Nils Blom Salmonsen <nbs@SBF.DK>; SBF - Johnny Restrup-Sørensen <jrs@sbf.dk>; Kristina Jæger <krj@oresundsbron.com>; Femern - Frederik Fisker <ffi@femern.dk>
Subject: VS: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Kære alle

Se vedlagte høring.

Venlig hilsen

Louise Friis
Juridisk konsulent
Ledelsessekretariatet

Dir.tlf. +45 33 41 62 41
Mobil +45 25 21 85 82

Sund & Bælt Holding A/S
Vester Søgade 10 Tel + 45 33 93 52 00 www.sundogbaelt.dk
1601 København V Fax + 45 33 93 10 25 www.storebaelt.dk

Fra: Bettina Karulf **På vegne af** Sund og Bælt
Sendt: 29. november 2017 15:06
Til: Søren Rosenkilde Clausen <src@sbf.dk>; Louise Friis <lfi@SBF.DK>
Emne: VS: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Venlig hilsen

Sund og Bælt

Sund & Bælt Holding A/S
Vester Søgade 10 Tel + 45 33 93 52 00 www.sundogbaelt.dk
1601 København V Fax + 45 33 93 10 25 www.storebaelt.dk

Fra: TRM Thea Bang Schou Jensen [mailto:tbj@TRM.dk]
Sendt: 29. november 2017 14:20
Emne: Høring vedr. forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren

Til høringsparterne

Hermed sendes forslag til Lov om sikkerhed i net- og informationssystemer i transportsektoren.

Udover forslag til ny lov sendes høringsbrev.

Høringsfristen er **tirsdag den 2. januar 2018, kl.10.00.**

Høringssvar til forslag til ny lov kan fremsendes pr. e-mail til trm@trm.dk med kopi til tbj@trm.dk

Bemærkninger og spørgsmål til lovforslaget bedes sendt til grh@trm.dk med kopi til jbn@trm.dk

Link til høringsportalen: https://hoeringsportalen.dk/Hearing/Details/61332

Venlig hilsen

Thea Bang Schou Jensen
Stud.jur

Transport-, Bygnings- og Boligministeriet
Ministry of Transport, Building and Housing
Internationalt Kontor
Frederiksholms Kanal 27 F
DK-1220 København K

Telefon: +45 72 26 71 46
tbj@trm.dk
www.trm.dk