FORSVARSMINISTERIET

26. maj 2021

Telerådsmøde den 4. juni 2021

Samlenotat

1. Forslag til direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 (KOM (2020) 823 endelig) **Fejl! Bogmærke er ikke defineret.**

1. FORSLAG TIL DIREKTIV OM FORANSTALTNINGER TIL SIKRING AF ET HØJT FÆLLES CYBERSIKKERHEDSNIVEU I HELE UNIONEN OG OM OPHÆVELE AF DIREKTIV (EU) 2016/1148 (KOM(2020) 823 ENDELIG)

Notatet er i sit indhold identisk med grund- og nærhedsnotatet, der blev oversendt til Folketingets Europaudvalg d. 15. februar 2021.

Forslaget er ikke omfattet af retsforbeholdet.

KOM(2020) 823 endelig

1. Resumé

Sagen er på dagsordenen på den uformelle videokonference for teleministre den 4. juni 2021 med henblik på formandsskabets præsentation af fremskridtsrapport.

Europa-Kommissionen (Kommissionen) har den 16. december 2020 fremsat forslag til direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 (KOM(2020) 823 final). Forslaget er modtaget i dansk sprogversion den 19. januar 2021.

Forslaget (NIS2) bygger på og ophæver direktiv (EU) 2016/1148 om sikkerhed i net- og informationssystemer (NIS-direktivet), som er den første EU-retsakt om cybersikkerhed og indeholder retlige foranstaltninger, der skal styrke det generelle cybersikkerhedsniveau i Unionen. Kommissionen har fremsat NIS2 på baggrund af en omfattende evaluering af NIS-direktivet gennemført i 2019 og 2020.

NIS2-forslaget tager fat på en række begrænsninger, der ifølge Kommissionen forhindrer NIS-direktivet i at indfri sit fulde potentiale. Forslaget indebærer derfor en væsentlig udvidelse af direktivets dækningsområde med flere sektorer herunder den statslige administration. Alle udbydere af tjenester inden for dækningsområdet omfattes af forslaget

(små virksomheder og mikrovirksomheder er som udgangspunkt undtaget). Der lægges op til væsentligt øgede krav til registrering af alle omfattede udbydere, samt væsentligt flere krav til de kompetente myndigheders tilsyn med udbyderne og udvidede sanktionsmuligheder ved brud på forpligtelserne vedrørende styring af cybersikkerhedsrisici og rapportering. Endelig indebærer forslaget udvidede krav til nationale cybersikkerhedsstrategier, krav om national cybersikkerhedskrisestyring, samt flere opgaver til det nationale centrale kontaktpunkt.

Regeringen ser overordnet positivt på forslaget og ønsket om at højne cybersikkerheden og trusselsbevidstheden - også i yderligere sektorer, der ikke traditionelt arbejder med sikkerhed. Udvidelsen af anvendelsesområdet, skærpede krav til risikostyring og rapportering samt det forudsatte myndighedstilsyn må generelt forventes at styrke cyberrobustheden, men det vurderes at være afgørende, at udvidelsen sker risikobaseret og proportionelt med respekt af sektoransvaret. Regeringen vil arbejde for, at forslaget ikke medfører uforholdsmæssige økonomiske byrder for aktører, som ikke er direkte afhængige af net- og informationssystemer, og at der arbejdes risikobaseret mhp. at balancere omkostningsniveau og merværdi. Endelig stillingtagen afventer en nærmere vurdering af de økonomiske konsekvenser, ikke mindst for nye sektorer, der omfattes af direktivet.

Sagen forelægges Folketingets Europaudvalg til orientering.

2. Baggrund

Forslaget kan ses som en videreførelse og udvidelse af bestemmelserne i det nuværende NIS-direktiv fra 2016 (2016/1148 (KOM(2020) 823 final).

Kommissionens konsekvensanalyse af det eksisterende NIS-direktiv konkluderede, at direktivet banede vejen for en betydelig ændring i tilgangen til cybersikkerhed både institutionelt og lovgivningsmæssigt i mange medlemsstater, men at det også har vist sine begrænsninger. Den digitale omstilling af samfundet (intensiveret af covid-19-krisen) har udvidet trusselsbilledet og skabt nye udfordringer, som kræver tilpassede og innovative sikkerhedsløsninger. Antallet af cyberangreb stiger fortsat, og der kommer stadig mere sofistikerede angreb fra en bred vifte af kilder i og uden for EU. Anvendelsesområdet for direktivet er ikke tilstrækkeligt klart, og medlemsstaterne har for vide skønsbeføjelser. Tilsyn og håndhævelses vurderes at være ineffektiv, ligesom modenheden i forbindelse med vurderingen af cybersikkerhedsrisici varierer for meget, og medlemsstaterne udveksler ikke systematisk oplysninger med hinanden.

Det er Kommissionens overordnede vurdering, at cybersikkerhed og -modstandsdygtighed på tværs af EU ikke kan være effektiv, hvis man

vælger en uensartet tilgang i form af løsrevne initiativer i nationale og regionale siloer.

NIS2 har til formål at styrke cyber sikkerheden og modstandsdygtigheden yderligere på en ensartet måde på tværs af medlemsstaterne, både i bredden og i dybden. Samtidig indgår NIS2 som en del af en bredere vifte af allerede eksisterende retlige instrumenter og af kommende initiativer på EU-plan, der i fællesskab har til formål at øge offentlige og private enheders modstandsdygtighed over for trusler og beredskabskapacitet inden for cybersikkerhed og beskyttelse af kritisk infrastruktur.

I forhold til fysisk sikkerhed supplerer forslaget Kommissionens forslag om revision af direktiv om kritiske enheders modstandsdygtighed (KOM(2020) 829 final)[1], som NIS2-forslaget er nøje afstemt med. Forslaget til direktiv om kritiske enheders modstandsdygtighed har til formål at styrke kritiske enheders modstandsdygtighed over for fysiske trusler i en lang række sektorer.

3. Formål og indhold

Kommissionen har den 16. december 2020 fremsat forslag til direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 (KOM(2020) 823 final). Forslaget er bygget op om en række centrale politikområder, som er indbyrdes forbundne og har til formål at højne cybersikkerhedsniveauet i Unionen.

Genstand og anvendelsesområde (artikel 1 og artikel 2)

Direktivet indeholder a) forpligtelser om, at medlemsstaterne skal vedtage en national cybersikkerhedsstrategi, udpege kompetente nationale myndigheder, centralt kontaktpunkt og CSIRT, b) bestemmelser om, at medlemsstaterne skal fastsætte forpligtelser om risikostyring og indberetning af cybersikkerhedshændelser for enheder, der benævnes "væsentlige", og c) bestemmelser om, at medlemsstaterne skal udveksle af oplysninger om cybersikkerhedshændelser.

Direktivet finder anvendelse på offentlige og private "væsentlige enheder", der opererer inden for de sektorer, som er opført i bilag I (energi, transport, bankvæsen, finansielle markedsinfrastrukturer, sundhed, drikkevand, spildevand, digital infrastruktur, offentlig forvaltning og rummet) og "vigtige enheder", der opererer inden for de sektorer, der er opført i bilag II (post- og kurertjenester, affaldshåndtering, fremstilling, fremstilling og distribution af kemikalier, fødevareproduktion, -

[1] Kommissionen fremsatte forslaget om direktiv om kritiske enheders modstandsdygtighed (KOM (2020) 829 final) d. 16. december 2020. Forslaget er modtaget i dansk sprogversion d. 9. februar 2021.

forarbejdning og -distribution, fremstillingsvirksomhed og digitale udbydere).

Det foreslåede anvendelsesområde betyder samlet set både en udvidelse af direktivets anvendelsesområde i bredden, såvel som i dybden. Således vil ikke kun nye sektorer indlemmes, men også langt flere virksomheder end i dag vil betegnes *væsentlige enheder*, som følge heraf. Det hidtidige princip om særskilt udpegning af udbydere af væsentlige tjenester i bestemte sektorer forlades, og der foreslås indført en højere grad af harmonisering af sikkerheds- og rapporteringsforpligtelser.

Mikrovirksomheder og små enheder som omhandlet i Kommissionens henstilling 2003/361/EF af 6. maj 2003 er ikke omfattet af direktivets anvendelsesområde, undtagen udbydere af elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, tillidstjenesteudbydere, topdomænenavneregistraturer, DNS-tjeneste-udbyder og offentlig forvaltning samt visse andre enheder såsom den eneste udbyder af en tjeneste i en medlemsstat. Derudover foreslås en mere lempelig ordning for efterfølgende tilsyn for de såkaldt "vigtige enheder" end de "væsentlige enheder". Hensigten er at minimere og afbalancere den byrde, der pålægges virksomheder og offentlige myndigheder.

Nationale rammer for cybersikkerhed (artikel 5-11)
Medlemsstaterne skal vedtage en national cybersikkerhedsstrategi, der definerer de strategiske mål og passende politiske og reguleringsmæssige foranstaltninger med henblik på at opnå og opretholde et højt cybersikkerhedsniveau.

Direktivet fastlægger også en ramme for koordineret indberetning af sårbarheder og pålægger medlemsstaterne at udpege CSIRT'er, der skal fungere som betroede formidlere og lette samspillet mellem de underrettende enheder og producenter eller udbydere af IKT-produkter og -tjenester. ENISA (EU's Agentur for Cybersikkerhed) skal udvikle og vedligeholde et europæisk sårbarhedsregister for de konstaterede sårbarheder.

Medlemsstaterne skal indføre nationale rammer for styring af cybersikkerhedskriser, bl.a. ved at udpege nationale kompetente myndigheder med ansvar for håndteringen af væsentlige cybersikkerhedshændelser og -kriser.

Medlemsstaterne skal også udpege en eller flere nationale kompetente myndigheder inden for cybersikkerhed til at varetage tilsynsopgaverne i henhold til dette direktiv og et nationalt centralt kontaktpunkt for cybersikkerhed (SPOC) til at varetage en forbindelsesfunktion for at sikre

grænseoverskridende samarbejde mellem medlemsstaternes myndigheder. Medlemsstaterne skal også udpege CSIRT'er.

NIS2-forslaget viderefører og udbygger således NIS-direktivets ramme: Der er allerede i dag i medfør af NIS etableret nationalt centralt kontaktpunkt og CSIRT ved Center for Cybersikkerhed, ligesom de sektoransvarlige myndigheder er kompetente myndigheder med ansvar for tilsynet med omfattede operatører og håndteringen af væsentlige cybersikkerhedshændelser og -kriser inden for deres respektive ansvarsområder.

Samarbejde (artikel 12-16)
Ved direktivet videreføres den samarbejdsgruppe, der skal støtte og lette det strategiske samarbejde og udvekslingen af oplysninger mellem medlemsstaterne og udvikle tillid. Der videreføres også det CSIRT-netværk, der skal bidrage til udviklingen af tillid mellem medlemsstaterne og fremme et hurtigt og effektivt operationelt samarbejde.

Med direktivet oprettes et europæisk netværk af cybersikkerhedsorganisationer (EU-CyCLONe), der skal støtte den koordinerede håndtering af væsentlige cybersikkerhedshændelser og -kriser og sikre regelmæssig udveksling af oplysninger mellem medlemsstaterne og EU-institutionerne.

ENISA skal i samarbejde med Kommissionen hvert andet år udsende en rapport om cybersikkerhedssituationen i Unionen.

Kommissionen skal etablere et evalueringssystem, der giver mulighed for regelmæssige *peer*-evalueringer af medlemsstaternes politikker for cybersikkerhed.

Forpligtelser vedrørende risikostyring og rapportering i forbindelse med cybersikkerhed (artikel 17-23)
I henhold til direktivet skal medlemsstaterne fastsætte bestemmelser om, at ledelsesorganer i alle enheder, der er omfattet af anvendelsesområdet, skal godkende de risikohåndteringsforanstaltninger vedrørende cybersikkerhed, der træffes af de respektive enheder, og følge specifik cybersikkerhedsrelateret uddannelse.

Medlemsstaterne skal sikre, at enheder inden for anvendelsesområdet træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at håndtere de cybersikkerhedsrisici, der er forbundet med sikkerheden i net- og informationssystemer. De skal også sikre, at enheder, både væsentlige og vigtige, underretter de nationale kompetente myndigheder eller CSIRT'erne om enhver cybersikkerheds-

hændelse, der har en væsentlig indvirkning på leveringen af den tjeneste, de udbyder. Som noget nyt, foreslås det også, at omfattede virksomheder skal indberette hændelser, som potentielt kunne have haft væsentlige konsekvenser.

Kommissionen kan vedtage gennemførelsesretsakter med henblik på at fastlægge mere detaljerede sikkerhedskrav samt i forbindelse med indberetning af væsentlige hændelser. Kommissionen tillægges endvidere beføjelser til at vedtage delegerede retsakter med henblik på at supplere sikkerhedskravene for at tage hensyn til nye cybertrusler, den teknologiske udvikling eller sektorspecifikke særtræk.

Topdomænenavneregistraturer og enheder, der leverer domænenavnsregistreringstjenester for topdomænet, indsamler og vedligeholder nøjagtige og fuldstændige oplysninger om domænenavnsregistrering samt offentliggør domæneregistreringsdata, som ikke er personoplysninger. Desuden er sådanne enheder forpligtet til at give lovlige adgangssøgende effektiv adgang til registreringsdata.

Kompetence og registrering (artikel 24 og 25)
Som hovedregel anses væsentlige og vigtige enheder for at være underlagt jurisdiktionen i den medlemsstat, hvor de leverer deres tjenester. Visse typer af enheder (udbydere af DNS-tjenester, topdomænenavneregistraturer, udbydere af cloud computing-tjenester, udbydere af datacentertjenester og udbydere af indholdsleveringsnetværk samt visse digitale udbydere) anses dog som udgangspunkt for at være underlagt jurisdiktionen i den medlemsstat, hvor foranstaltninger til styring af cybersikkerhedsrisici træffes.

Dette skal sikre, at sådanne enheder ikke stilles over for en lang række forskellige retlige krav, eftersom de i særlig høj grad leverer tjenesteydelser på tværs af grænserne. ENISA skal oprette og føre et register over den sidstnævnte type enheder.

Udveksling af oplysninger (artikel 26 og 27)
Medlemsstaterne fastsætter regler, der gør det muligt for enheder at deltage i udveksling af cybersikkerhedsrelaterede oplysninger inden for rammerne af specifikke ordninger for udveksling af cybersikkerhedsoplysninger i overensstemmelse med artikel 101 i TEUF.

Desuden tillader medlemsstaterne enheder, der ikke er omfattet af dette direktiv, frivilligt at foretage underretninger om væsentlige hændelser, cybertrusler eller nærvedhændelser.

Tilsyn og håndhævelse (artikel 28-34)

De kompetente myndigheder skal føre tilsyn med de enheder, der er omfattet af direktivet, og navnlig sikre, at de overholder kravene til sikkerhed og underretning om hændelser. Der skelnes mellem en forudgående tilsynsordning for væsentlige enheder og en ordning for efterfølgende tilsyn med vigtige enheder, idet det senere kræves, at de kompetente myndigheder træffer foranstaltninger, når de får forelagt dokumentation for eller tegn på, at en vigtig enhed ikke opfylder kravene til sikkerhed og underretning om hændelser.

Direktivet pålægger også medlemsstaterne at sikre, at de kompetente myndigheder har beføjelse til at pålægge eller anmode f.eks. domstolene om pålæggelse af administrative bøder til væsentlige og vigtige enheder og fastsætter visse maksimumsbøder. Det vil skulle afklares nærmere, hvordan direktivets bestemmelser om at give kompetente myndigheder beføjelse til at pålægge eller anmode om at pålægge administrative bøder, nærmere skal forstås.

Medlemsstaterne skal samarbejde og bistå hinanden efter behov, når enheder leverer tjenesteydelser i mere end én medlemsstat, eller når en enheds hovedvirksomhed eller dens repræsentant er beliggende i en bestemt medlemsstat, mens dens net- og informationssystemer er beliggende i en eller flere andre medlemsstater.

4. Europa-Parlamentets udtalelser

Europa-Parlamentet er i henhold til den almindelige lovgivningsprocedure (TEUF art. 294) medlovgiver. Der foreligger endnu ikke en udtalelse.

Det er Europa-Parlamentets udvalg for industri, forskning og energi (ITRE), der behandler forslaget.

5. Nærhedsprincippet

Det er Kommissionens vurdering, at modstandsdygtigheden over for cybertrusler i hele Unionen ikke er effektiv, hvis der gribes ind på en uensartet måde gennem nationale eller regionale siloer. NIS-direktivet afhjalp til dels denne mangel ved at fastlægge en ramme for net- og informationssystemernes sikkerhed på nationalt plan og EU-plan.

Ifølge Kommissionen har medlemsstaternes uens implementering peget på, at den eksisterende NIS-direktiv er begrænset ift. at kunne indfri målet om et højt fælles cyber- og informationssikkerhedsniveau, herunder som følge af det nuværende direktivs anvendelsesområde. Siden covid-19-krisen er den europæiske økonomi desuden blevet endnu mere afhængig af net- og informationssystemer end nogensinde før, og sektorer og tjenester er i stigende grad indbyrdes forbundne.

Kommissionen begrunder på den baggrund en EU-indsats, der går videre end det nuværende NIS-direktivs foranstaltninger i: i) cybertruslen og udfordringernes stadig mere grænseoverskridende karakter, ii) potentialet i Unionens indsats med hensyn til at forbedre og fremme effektive og koordinerede nationale politikker og iii) bidraget fra samordnede og samarbejdsbaserede politiske tiltag til effektiv beskyttelse af personoplysninger og privatlivets fred.

På det foreliggende grundlag er det regeringens vurdering, at nærhedsprincippet er overholdt.

6. Gældende dansk ret

Implementeringen af det nugældende NIS-direktiv er gennemført via en række love og bekendtgørelser inden for de nuværende involverede respektive ministerområder. Implementeringen er sket efter sektoransvarsprincippet, hvorefter de sektoransvarlige myndigheder er kompetente myndigheder i direktivets forstand og har implementeret direktivet i relevant lovgivning på deres områder. Denne decentrale hjemlige implementering har først og fremmest fokus på det eksisterende direktivs forpligtelser for "operatører af væsentlige tjenester" og "udbydere af digitale tjenester". Begge begreber forlades med NIS2.

I det følgende opridses den nationale lovgivning iht. det nugældende direktiv inden for de respektive ressortministerier.

Erhvervsministeriets område
Lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester (LOV nr. 436 af 437 af 08/05/2018), stiller krav om sikkerhed og underretningspligt for topdomænenavnsadministratorer, DNS-tjenesteudbyder (DNS – Domænenavnesystem), udbydere af onlinemarkedspladser, udbydere af onlinesøgemaskine og udbydere af cloud computing-tjenester. Loven stiller desuden disse krav for den finansielle sektor.

Bekendtgørelse om sikkerhed i net- og informationssystemer af betydning for skibes sikkerhed og deres sejlads (BEK nr. 46 af 16/01/2019) fastsætter bestemmelser og stiller krav til maritime operatører om sikkerhed i net- og informationssystemer, som anvendes i leveringen af maritime tjenester.

Forsvarsministeriets område
Lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. (LOV nr. 437 af 08/05/2018) stiller krav om sikkerhed og underretningspligt for internetudvekslingspunkter (Internet Exchange Points – IXP), som alene er de udbydere, der angår informationssikkerhed under Forsvarsministeriet.

Herudover skaber loven forudsætningerne for, at Center for Cybersikkerhed kan varetage funktionerne som beredskabsenhed, der skal håndtere it-sikkerhedshændelser (CSIRT), og som nationalt centralt kontaktpunkt.

Klima-, Energi og Forsyningsministeriets område
Net- og informationssikkerhedsdirektivet er inden for energisektoren blevet implementeret ved § 85 c i lov om elforsyning og § 15 b i lov om naturgasforsyning, hvor ministeren bemyndiges til at udstede nærmere regler. Disse bemyndigelser er udmøntet i bekendtgørelse nr. 820 af 14. august 2019 om it-beredskab i el- og naturgassektorerne. NIS-direktivet er ligeledes implementeret i bekendtgørelse nr. 424 af 25. april 2018 om beredskab for oliesektoren.

Disse stiller krav om sikkerhed, beredskab og underretningspligt for virksomheder med el-produktionsbevilling, virksomheder med netbevilling, el- og naturgas-transmissionsoperatører, balanceansvarlige virksomheder, virksomheder som holder olieberedskabslagre i Danmark og virksomheder som har naturgaslagre i Danmark.

Miljøministeriets område
Direktivet er implementeret på drikkevandsområdet med bkg. nr. 429 af 04/05/2018 om krav til sikkerheden i visse vandforsyningers net- og informationssystemer.

Sundhedsministeriets område
Lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren (LOV nr. 440 af 08/05/2018) stiller krav om sikkerhed og underretningspligt for operatører af væsentlige tjenester inden for sundhedssektoren.

Bekendtgørelse om operatører af væsentlige tjenester (BEK 458 af 09/05/2018) opstiller kriterier for identifikation af operatører af væsentlige tjenester i sundhedssektoren og definerer krav til deres sikkerhedsforanstaltninger, registrering og underretningspligt*. Bekendtgørelse om delegation af opgaver fra sundhedsministeren til Sundhedsdatastyrelsen* (BEK 459 af 09/05/2018) delegerer NIS-opgaver til Sundhedsdatastyrelsen, herunder bl.a. tilsyn med operatører af væsentlige tjenester.

Transportministeriets område
Lov om sikkerhed i net- og informationssystemer i transportsektoren (Lov nr. 441 af 8. maj 2018) samt bekendtgørelse om sikkerhed i net- og

informationssystemer i transportsektoren (Bekendtgørelse nr. 1042 af 6. august 2018) implementerer det nuværende NIS-direktiv i transportsektoren.

Derudover eksisterer der i sektoren EU-sektorlovgivning, som har til formål at sikre et højt cybersikkerhedsniveau. En række nye cybersikkerhedsregler inden for civil luftfart træder desuden i kraft i de kommende år, herunder forordning (EU) nr. 2019/1583 inden for security-området (i 2021), og i 2022 følger nye EU-regler inden for safety-området.

7. Konsekvenser

Lovgivningsmæssige konsekvenser

Implementering af direktivet vil kræve ændring i den ovennævnte lovgivning i sektorerne, ligesom det vil skulle etableres lovhjemmel i nye sektorer.

Økonomiske konsekvenser

Forslaget vurderes at have statsfinansielle konsekvenser samt erhvervsøkonomiske konsekvenser. Disse kan ikke nærmere kvantificeres på nuværende tidspunkt. Fra dansk side udestår således en nærmere vurdering af de statsfinansielle konsekvenser samt de erhvervsøkonomiske konsekvenser herunder administrative konsekvenser og øvrige efterlevelseskonsekvenser, herunder særligt i de nye sektorer.

De administrative konsekvenser består i, at danske virksomheder i forbindelse med implementeringen af direktivet i dansk ret vil blive pålagt potentielt væsentlige administrative byrder. Det skyldes, at der i direktivet sker en udvidelse af definitionen af væsentlige udbydere og krav i forhold til i dag, hvilket betyder, at flere virksomheder fremadrettet vil blive omfattet af definitionen og de administrative krav det medfører. De administrative byrder indebærer bl.a. tilsyn, registrerings- og rapporteringsforpligtelser, idet virksomhederne skal indberette hændelser, og evt. certificering.

De administrative konsekvenser ved ovenstående kan ikke nærmere kvantificeres på nuværende tidspunkt.

Ifølge Kommissionen vil forslaget medføre visse overholdelses- og håndhævelsesomkostninger for de relevante myndigheder i medlemsstaterne (anslået samlet stigning på ca. 20-30 % af ressourcerne). Kravet til myndighederne om at føre et udfoldet tilsyn og øget kontrol med enhederne omfattet af direktivet vil i sig selv indebære et væsentligt forøget ressourceforbrug for de sektorer, som ikke fører et tilsyn med net- og informationssikkerhed under den nuværende lovgivning.

Kommissionen anslår, at for de virksomheder, der vil være omfattet af NIS2-forslaget, vil deres nuværende udgifter til sikkerhed til informations- og kommunikationsteknologi (IKT) skulle øges med 22 % i de første år efter indførelsen af NIS2-forslaget (dette vil være 12 % for virksomheder, der allerede er omfattet af det nuværende NIS-direktiv). Små virksomheder og mikrovirksomheder er som udgangspunkt undtaget fra NIS2-forslaget.

Andre konsekvenser og beskyttelsesniveauet
Forslaget vurderes at have positive konsekvenser for cybersikkerheden og trusselsbevidstheden og kunne reducere omkostningerne ved cybersikkerhedshændelser.

Ifølge Kommissionen vil NIS2-forslaget medføre betydelige sikkerhedsmæssige fordele takket være et bedre overblik over og interaktion med centrale virksomheder, øget grænseoverskridende operationelt samarbejde samt gensidig bistand og peer-evalueringsmekanismer. Dette vil føre til en generel forøgelse af cybersikkerhedskapaciteterne på tværs af medlemsstaterne. Samtidig vil en styrkelse af sikkerhedsniveauet tilskynde de involverede udbydere til at styrke deres cybersikkerhedskapaciteter og bidrage til en forbedring af udbydernes IKT-risikostyring.

Ifølge Kommissionen vil den ovenfor beskrevne gennemsnitlige stigning i udgifterne til IKT-sikkerhed medføre en forholdsmæssig fordel ved sådanne investeringer, navnlig på grund af en betydelig reduktion af omkostningerne ved cybersikkerhedshændelser (som af Kommissionen anslås til 11,3 mia. EUR over 10 år).

8. Høring

Forslaget er sendt i høring d. 19. januar 2021 i specialudvalget for civilbeskyttelse, specialudvalget for konkurrenceevne, vækst og forbrugerspørgsmål, specialudvalget for transport, skibsfartspolitisk specialudvalg, specialudvalget for klima-, energi- og forsyningspolitik EU-landbrugsudvalget (§2-udvalget), EU-fiskeriudvalget (§5-udvalget) og Det Rådgivende Fødevareudvalgs EU-undervalg med frist d. 3. februar 2021. Der er modtaget hørringssvar fra Akademikerne, Danske Havne, Danske Maritime, Dansk Industri, Dansk Standard, Dansk Vand- og Spildevandsforening, Danske Rederier og Færgerederierne, Danske Regioner, Dansk Erhverv / IT Branchen, Danske Statsbaner, Erhvervsflyvningens Sammenslutning, Finans Danmark, Forsikring og Pension, Ingeniørforeningen (IDA), Kommunernes Landsforening, Landbrug & Fødevarer, Teleindustrien.

Generelle bemærkninger

Akademikerne (AC) er generelt positive overfor tiltag, som kan styrke niveauet for cybersikkerheden i Danmark og andre europæiske lande, der jævnligt rammes af angreb fra forskellige typer aktører, såvel som data-læk grundet menneskelige fejl som følge af manglende kompetencer eller opmærksomhed, idet at **AC** finder at dette har store konsekvenser for de enkelte virksomheders økonomi, samfundets forsyningssikkerhed, statens sikkerhed og almindelige borgeres tillid til et stadigt mere digitalt samfund. Derfor er **AC** enige i formålet med forslaget, og er også enige i, at en stor del af indsatsen for et højere sikkerhedsniveau sker på europæisk plan, dvs. i regi af EU.

AC finder det positivt, at der grundet den stigende dataudveksling, med forslaget sker en stramning i forhold til at udligne forskelle mellem de europæiske lande, samt at alle lande løftes til et forsvarligt niveau. Samtidig finder **AC** det fornuftigt, at stramninger sker med forståelse for, hvad der kan lade sig gøre og hvilke tiltag der er mest effektive i forhold til, hvilke typer organisationer og virksomheder, der stilles krav til. **AC** vurderer, at det derfor giver mening at stille andre (og muligvis mindre) krav til mikrovirksomheder og start-ups end til store virksomheder og offentlige organisationer, så kravene følger proportionalitetsprincippet.

AC bemærker, at et stigende cybersikkerhedsniveau må medføre omkostninger for virksomheder og offentlige organisationer, især på kort sigt, og at en forbedring af sikkerhedsniveauet, ofte kræver en indsats i forhold til håndhævelse af regler, kompetenceopbygning samt en opgradering af forældede eller usikre it-systemer, der ikke er udviklet med henblik på at yde sikkerhed mod fejl eller angreb. **AC** vurderer, at omkostningerne dog må forventes at blive opvejet af fordele som færre omkostninger ved hackerangreb for de enkelte virksomheder og organisationer, mere effektiv digitalisering i de europæiske samfund generelt, mindre behov for krisehåndtering, en mere it-kompetent arbejdsstyrke og en større tryghed ved digitalisering hos borgerne, når deres personlige data opbevares sikkert og beskyttet. **AC** finder, at særligt borgernes tryghed i forhold til datahåndteringen og sikkerheden ved dette, er vigtig at holde fast i og styrke.

Danske Havne (DH) støtter, at indsatsen mod cyberkriminalitet skal tilpasses og styrkes for at sikre vigtig infrastruktur. **DH** bemærker vigtigheden af, at de forpligtelser, som direktivet pålægger virksomheder (i dette tilfælde havne), der betragtes som vigtig infrastruktur, er proportionale med truslen fra cyberkriminalitet, og at dette gælder både i forhold til omkostningerne og den administrative byrde for havnene.

DH bemærker, at mindre virksomheder (mindre end 50 ansatte) ikke er omfattet af kravene til cybersikkerhed, men at det dog er usikkert, om det førnævnte også gælder for havne, idet at direktivet henviser til havne som defineret i sikringsdirektivet, hvilket stort set dækker alle danske erhvervshavne - også de meget små. **DH** ønsker derfor at sikre, at størrelsen af havnene også tages i betragtning, da det alternativt kan medføre store ekstraomkostninger for små havne.

DH anfører vigtigheden af, at der foretages en cybersikkerhedsvurdering, inden en havn er underlagt alle foranstaltningerne i direktivet.

DH bemærker, at det ofte ikke er havnen som sådan, der driver al kritisk infrastruktur i havnen, f.eks. containerterminaler og færgeterminaler, og derfor ikke havnen, der skal være genstand for foranstaltningerne. **DH** foreslår derfor, at evalueringen af, om en havn skal være underlagt reglerne i direktivet, foretages individuelt og af den kompetente nationale myndighed. Den nationale myndighed bør foretage en specifik risikovurdering af hver havn og på dette grundlag beslutte, om den skal være omfattet af kravene til kritisk infrastruktur i direktivet, og at det også skal specificeres, hvilke dele af havnen (systemer osv.) der i så fald betragtes som kritisk infrastruktur.

DH bemærker, at forslaget vil medføre store ekstraomkostninger til implementering og vedligeholdelse, og foreslår på denne baggrund, at der er mulighed for økonomisk støtte til de virksomheder / havne, der er omfattet af kravene.

Danske Maritime (DM) bemærker, at antallet og karakteren af cyberangreb er bekymrende, idet der kommer stadig mere sofistikerede angreb fra en bred vifte af kilder i og uden for EU. **DM** lægger derfor vægt på indgåelse af effektive internationale aftaler vedr. cybersikkerhed, og støtter op om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele EU.

Dansk Industri (DI) bemærker, at hastigheden, som samfundet digitaliseres i, og erfaringerne fra det eksisterende NIS-direktiv, retfærdiggør det nye forslag, som et led i EU's bestræbelser på at skabe den nødvendige cybersikkerhed i unionen. **DI** henviser samtidig til de omfattende skadesvirkninger af hackerangreb og cyberkriminalitet, samt COVID-19 pandemiens tydeliggørelse af digitaliseringens betydning for samfundet, som eksempler på at digitalisering bør ske med et nødvendigt fokus på cybersikkerhed. **DI** bifalder derfor Kommissionens prioritering af cybersikkerhed, og finder det positivt, at forslaget bygger på en ensartet tilgang blandt myndigheder, organisationer og

virksomheder i Europa, således at virksomhederne fremadrettet undgår uens krav til cybersikkerhed i de forskellige EU-medlemslande.

DI bemærker, at forslaget vil give de valgte kompetente myndigheder store beføjelser i forhold til at pålægge virksomheder efterlevelse af forskellige krav til cybersikkerhed, og til at pålægge virksomhederne administrative bøder på op til 10.000.000 EUR eller op til 2 % af virksomhedens årsomsætning, alt efter hvad der er højest. **DI** vurderer, at selv om der i direktivforslaget er tale om en halvering af de maksimale bødestørrelser i GDPR-regi, er der tale om potentielle massive bøder til virksomheder, der ikke overholder forpligtelserne i direktivet.

DI sætter spørgsmålstegn ved om massive bødestørrelser er den rigtige vej at gå på et område som cybersikkerhed, der er styret af risikovurderinger, og hvor passende tiltag er og skal være dynamiske for at tilpasse sig det skiftende trusselsbillede og den teknologiske udvikling, hvortil **DI** bemærker at sidstnævnte tillige er afspejlet i direktivets overordnede formuleringer til virksomhedernes forpligtelser.

DI bemærker yderligere, at de kompetente myndigheder gives mulighed for at pålægge virksomhederne en række indgreb som led i tilsyn og håndhævelse af direktivet. Samtidig ser **DI** en risiko for, at truslen om massive bøder skaber frygt for at anvende data, at digitalisere og at skabe værdi gennem digital nytænkning på samme måde, som **DI** har set, og fortsat ser, i kølvandet på implementeringen af GDPR.

DI ser det som helt afgørende, at den nationale implementering af direktivet sker med et klart udgangspunkt i proportionalitet og risikovurderinger, og bemærker, at dialog og samarbejde giver erfaringsmæssigt bedre resultater end krav og bøder, som risikerer at føre til et større fokus på compliance, fremfor indtænkning af cybersikkerhed i forretningen og en reel styrkelse af cybersikkerheden.

DI bemærker, at Kommissionen foreslår, at NIS2 også kommer til at omfatte en række vigtige "important" sektorer, herunder "manufacturing", hvilket indebærer, at lovforslaget i modsætning til tidligere lovgivning om infrastruktur også kommer til at omfatte f.eks. maskiner og elektriske produkter i værdikæden. **DI** finder, at det er problematisk, at det samme problem søges løst mange forskellige steder på samme tid. DI er bekymret for, at det resulterer i, at samme produkt pålægges flere forskellige og evt. modsatrettede krav; og så gerne, at krav vedr. produkters cybersikkerhed, blev harmoniseret som anden produktlovgivning.

DI bemærker, at CSA ikke baserer sig på principperne bag NLF, og finder det derfor ikke hensigtsmæssigt, at NIS2 refererer til brug af standarder under CSA. Obligatorisk anvendelse af standarder udviklet under CSA af 3. part, og dermed obligatorisk certificering, vil være et brud med NLF og påfører virksomhederne unødvendige administrative og økonomiske byrder. **DI** finder at det bør være muligt for virksomheder frit at vælge, hvordan de ønsker at opfylde de krav til cybersikkerhed, som deres produkter er underlagt, og i det omfang de ønsker det, på frivillig basis, benytte de relevante standarder eller state-of the art teknologier, der sikrer kravenes opfyldelse, idet at det er således for alle andre risici, og **DI** ikke ser nogen grund til at fravige dette princip for cybersikkerhed.

DI bemærker, at i det omfang virksomhederne anvender harmoniserede standarder, opnås fri bevægelighed indenfor EU. I det omfang, at lovgiverne mener, at produktgruppen skal inddrage 3.part i deres risikovurdering og overensstemmelsesvurdering, inddrages 3.part. Ikke med henblik på certificering, men med henblik på at færdiggøre overensstemmelseserklæringen og påføre produktet dets CE-mærkning.

Dansk Standard (DS) stiller sig generelt positivt overfor udspillet fra Kommissionen, og finder ligeledes at direktivudkastet overordnet fint løser de udfordringer, der er påpeget i evalueringen af det nuværende direktiv.

Dansk Vand- og Spildevandsforenings (DANVA) mener overordnet set, at der skal være de lovgivningsmæssige rammer, der sikrer og understøtter, at danske virksomheder arbejder effektivt med informations- og cybersikkerhed – udfra en risikobaseret tilgang. **DANVA** finder, at udkastet til direktiv vil være med til at forbedre rammerne for informations- og cybersikkerhedsarbejdet i forsyningsselskaberne.

DANVA bemærker, at der ikke er angivet nogle vandforsyninger på NIS-bekendtgørelsens bilagsliste og, at der i praksis ikke er nogen danske erfaringer med NIS-direktivet. **DANVA** understreger, at informations- og cybersikkerhedsindsatsen skal være passende og proportional i forhold til risikosituationen og omkostningerne.

DANVA bemærker det typisk vil være vandselskaber af en vis størrelse, der bliver omfattet. **DANVA** bemærker hertil, at denne form for arbejde kræver stor viden og mange ressourcer. **DANVA** anfører, at der er behov for yderligere uddybning af anvendelsesområdet, da det ikke er velbeskrevet, om en række micro- og små vandselskaber kan blive omfattet i visse situationer.

DANVA finder, at det er afgørende, at der etableres et frugtbart og velfungerende, dialogbaseret samarbejde mellem regulator, myndigheder og selskaberne, og at samarbejdet bør tage udgangspunkt i selskabernes informations- og cybersikkerhedssituation. **DANVA** byder det tværsektorielle samarbejde velkommen og opfordrer generelt til videndeling, udsendelse af advarsler og operationel information.

DANVA bemærker, at tvangsindgreb kun bør anvendes, hvis mindre indgribende foranstaltninger ikke er tilstrækkelige, og hvis indgrebet står i rimeligt forhold til formålet med indgrebet. **DANVA** bemærker, at der er behov for yderligere afklaring af hvilke omkostninger – direkte som indirekte – direktivet vil afstedkomme for vandselskaberne.

Danske Rederier og Færgerederierne (DRFR) ser ikke behov for en større revision af direktivet for sektoren, idet **DRFR** finder, at det eksisterende NIS-direktiv ((EU) 2016/1148) har opfyldt sit formål med hensyn til søtransport. **DRFR** bemærker hertil, at der på skibsfartsområdet er lex specialis og derfor ikke behov for at der stilles forøgede krav til shipping og logistik virksomheder i forbindelse med NIS2.

DRFR finder, at forslaget synes at foreslå en mere central tilgang både nationalt og på EU-plan. **DRFR** understreger her den danske decentrale tilgang til cybersikkerhed, baseret på sektoransvarsprincippet, som **DRFR** støtter.

DRFR støtter fuldt ud, at små- og mikrovirksomheder er undtaget fra forslaget. **DRFR** bemærker samtidigt, at det er vigtigt, at øvrige virksomheder ikke automatisk bliver en del af direktivet. Dette skal i stedet bero på at den ansvarlige sektormyndighed i medlemsstaterne identificere omfattede virksomheder.

DRFR bemærker, at de foreslåede tekniske og organisatoriske foranstalt-ninger kan være meget omfattende og dyre for en virksomhed eller enhed at gennemføre, hvorfor der skal gives tilstrækkelig tid til implementering.

Danske Regioner (DKR) er enige i direktivets grundlæggende præmis; at øge cybersikkerheden på tværs af EU og ensrette krav til operatører i de samfundskritiske sektorer. **DKR** finder det positivt, at der i forslaget er indarbejdet et større fokus på og sammenhæng med de europæiske databeskyttelsesregler, så det bliver mere entydigt i praksis.

DKR bemærker forslagets muligheder for håndhævelsesforanstaltninger, sanktioner og administrative bøder ved manglende efterlevelse af direktivet. **DKR** anbefaler, at man ser på hvilke virkemidler, der er de

mest hensigtsmæssige til at fremme formålet. **DKR** bemærker, at en fælles udvikling kræver en vis åbenhed om fejl og mangler, og at bøder kan modvirke den mekanisme.

DKR konstaterer, at direktivet beskriver, at pålagte tilsyns- og håndhævelsesforanstaltninger skal have en "afskrækkende virkning". **DKR** bemærker, at det afviger markant fra den samarbejdsorienterede tilgang de danske sundhedsmyndigheder har lagt op til frem til nu. **DKR** anbefaler, at det gøres let og risikofrit at indberette cybertrusler og hændelser frem for, at aktørerne risikerer strengere tilsyn og pålagte foranstaltninger med "afskrækkende virkning".

DKR bemærker, at der ikke er en tydelig sammenhæng mellem formålet om at styrke cybersikkerheden og de hændelser, der skal underrettes om. **DKR** finder, at det er utydeligt, hvornår en hændelse er så væsentlig, at den skal indberettes. **DKR** anbefaler, at der som minimum udformes supplerende beskrivelser, der tydeliggør og konkretiserer hvilke hændelser, der skal underrettes om. **DKR** bemærker, at forslaget rummer mange nye opgaver med deraf et stort afledt ressourcetræk. **DKR** bemærker hertil, at der er behov for at vurdere de samlede konsekvenser af forslaget.

Dansk Erhverv / IT-Branchen (DEIT) støtter til fulde hensigten bag NIS2. Virksomheder kan lide meget store økonomiske tab i tilfælde af it-sikkerhedshændelser, som det er sket for flere markante danske virksomheder i de seneste år. Desuden er der store samfundsmæssige risici forbundet med angreb på særligt de kritiske samfundssektorer.

DEIT har i regi af den nuværende NIS-ramme været involveret i nedsættelsen af en decentral cyber- og informationssikkerhedsenhed (DCIS) i telesektoren. **DEIT** bemærker hertil, nedsættelse og drift af en DCIS er en betydelig ressourcekrævende opgave for de berørte virksomheder, organisationer og myndigheder. Til gengæld giver samarbejdet en række sikkerhedsmæssige fordele i form af nyttig udveksling af viden og mulighed for hurtigere reaktioner på trusler.

DEIT bemærker de i Kommissionens konsekvensanalyse angivne øgede omkostninger for nuværende og fremtidige omfattede virksomheder, samt de øgede offentlige udgifter. **DEIT** bemærker hertil de af Kommissionen skønnede besparelser. **DEIT** opsummerer i forlængelse heraf, at det afgørende er, at indsatsen målrettes de virksomheder, der i kraft af deres størrelse og rolle i samfundet, har tilstrækkelig betydning til, at omkostningerne står i proportion til udfordringernes karakter.

Danske Statsbaner (DSB) vurderer generelt, at direktivforslaget indeholder mange gode aspekter i forhold til styrkede krav til risikostyring, mere samarbejde og løbende opfølgning. DSB ser dog samtidigt aspekter i forslaget, som kan have den effekt, at der skabes meget stor fokus på compliance og formel rapportering og derved mindre fokus på den operationelle tekniske styring af cybersikkerhedsrisici.

Erhvervsflyvningens Sammenslutning (ES) bemærker, at der i konsekvensanalysen konkluderes, at den foretrukne løsningsmodel er løsningsmodel 3 (systemiske og strukturelle ændringer af NIS-rammen). **ES** kan støtte løsning 3, som den fremgår af konsekvensanalysens konklusion, men har herudover ikke yderligere bemærkninger.

Finans Danmark (FD) finder det positivt, at Kommissionen fastholder fokus på et højt sikkerhedsniveau for de europæiske samfundskritiske funktioner og digitale infrastrukturer. **FD** finder det positivt, at Kommissionens forslag udvider anvendelsesområdet ved at tilføje nye sektorer baseret på deres kritiske indflydelse på økonomien og samfundet. **FD** finder det videre positivt, at der indføres et klart størrelsesloft - hvilket betyder, at alle mellemstore og store virksomheder i udvalgte sektorer vil blive omfattet. **FD** bemærker, at det er vigtigt, at det er entydigt, hvem der er omfattet.

FD bemærker, at den eksisterende NIS-rammes sondring mellem operatører af væsentlige tjenester og udbydere af digitale tjenester fjernes, til fordel for en klassifikation på baggrund af betydning i hhv. væsentlige og vigtige kategorier med den konsekvens, at de underkastes forskellige tilsynsordninger. **FD** anbefaler, at der her sigtes mod en differentiering baseret på et proportionalitetsprincip, således at relevante krav målrettes den faktiske risiko. **FD** finder det positivt, at forslaget styrker sikkerhedskrav ved at indføre krav om en risikostyringstilgang.

FD bemærker, at der oprettes et antal nye organer (f.eks. Den fælles cyberenhed). **FD** bemærker hertil, at det er vigtigt at undgå overlappende ansvar, især mellem nationale organer og overnationale organer. **FD** anbefaler, at der er fokus på ikke at skabe et meget komplekst, fragmenteret og besværligt rapporterings-økosystem. **FD** bemærker bestemmelserne vedrørende IKT-certificering og finder, at det både er positivt og proportionalt, at det er leverandøren, der skal sikre, at sikkerheden er på plads gennem en certificeringsordning.

FD bemærker, at finanssektoren i tillæg til NIS2 også forventes omfattet af DORA ("Digital Operational Resilience Act"), der bliver en Lex specialis for finansielle institutioner/finansmarkedets infrastruktur. **FD** finder det afgørende, at der i den forbindelse undgås dobbeltregulering eller skabes usikkerhed. **FD** bemærker videre, at der i direktivet om

kritiske enheders modstandsdygtighed henvises til cyber- og ikke-cybermodstandsdygtighed. **FD** finder det også afgørende, at der også i denne forbindelse undgås dobbeltregulering eller skabes usikkerhed.

FD bemærker, at finanssektoren er underlagt en række rapporteringskrav på cybersikkerhedsområdet, og forventes i fremtiden at blive underlagt flere rapporteringskrav. **FD** anbefaler, at rapporteringskrav i videst muligt omfang harmoniseres.

Forsikring og Pension (F&P) giver stor opbakning til en mere fokuseret indsats, der bidrager til at øge modstandsdygtigheden over for cyberangreb i den finansielle sektor i EU og Danmark. **F&P** bemærker at cybersikkerhedsdagsordenen i forvejen er højt prioriteret i den danske forsikrings- og pensionsbranche, hvor der er tæt koordinering og videndeling.

F&P har i efteråret 2020 givet høringssvar på EU's lovforslag til "Digital Operationel Resilience Act (DORA)", som kommer til at regulere den finansielle branche.

F&P foreslår derfor, at det bliver tydeliggjort i selve lovteksten i NIS-direktivet (og ikke kun i præamblen pkt. 13), at direktivet ikke gælder for forsikrings- og pensionsbranchen, så der fremadrettet ikke er tvivl om, hvilke krav finansielle virksomheder skal efterleve.

Ingeniørforeningen IDA (IDA) er overordnet positiv overfor direktivet. Som årsag anføres fokus på et styrket niveau af cybersikkerhed i Danmark og andre europæiske lande, der jævnligt rammes af cyberangreb så vel som datalæk grundet menneskelige fejl som følge af manglende kompetencer eller opmærksomhed.

IDA vurderer at cyberangreb og datalæk har store konsekvenser for de enkelte virksomheders økonomi, samfundets forsyningssikkerhed, statens sikkerhed og almindelige borgeres tillid til et stadigt mere digitalt samfund.

IDA anfører, at manglende cybersikkerhed kan være meget lokalt og angreb eller fejl kan ramme meget specifikt, imens digitaliseringen generelt er international og udveksling af data flyder konstant mellem EU-landene. **IDA** er derfor varm fortaler for, at en stor del af indsatsen for et højere sikkerhedsniveau sker på europæisk plan, dvs. i regi af EU. **IDA** angiver vigtigheden af, at forskelle mellem de europæiske lande udlignes og løftes til et forsvarligt niveau, og finder det fornuftigt at stramningerne sker ved at stille differentierede krav til ex. hhv.

store organisationer og hhv. mikrovirksomheder, baseret på forståelsen af, hvad der kan lade sig gøre, og hvilke tiltag som er mest effektive, i forhold til den pågældende organisation.

Samtidig finder **IDA**, at de på kort sigt højnede omkostninger for offentlige organisationer og virksomheder, til at etablere et stigende cybersikkerhedsniveau, må forventes at blive opvejet af fordele, så som færre omkostninger ved hackerangreb; mere effektiv digitalisering i de europæiske samfund generelt; mindre behov for krisehåndtering; en mere it-kompetent arbejdsstyrke; og en større tryghed ved digitalisering hos borgerne, når deres personlige data opbevares sikkert og beskyttet.

Kommunernes Landsforening (KL) finder, at der er mange gode initiativer i direktivet, som kan medvirke til fælles tiltag på cybersikkerhedsområdet. Generelt finder KL, at der er behov for koordinering med de krav der følger af GDPR ift. både risikovurderinger, fastsættelse af krav til udveksling af oplysninger og håndtering af udfordringer med manglende overholdelse.

Landbrug & Fødevarer (LF) bemærker, at Fødevareklyngen har mange virksomheder med få ansatte. **LF** finder det derfor positivt og proportionelt, at små virksomheder og mikrovirksomheder vil blive undtaget fra NIS-rammens anvendelsesområde. **LF** bemærker den af Kommissionen anslåede forøgelse af omkostninger på 22 % i de første år efter indførelsen af den nye NIS-ramme. **LF** finder, at dette er uproportionalt og en markant erhvervsøkonomisk konsekvens.
LF bemærker overholdelses- og håndhævelsesomkostninger for de relevante myndigheder i medlemsstaterne, og den af Kommisionen anslåedesamlede stigning på ca. 20-30 % af ressourcerne. **LF** udtrykker bekymring for den øgede omkostningsbyrde for de relevante myndigheder.

LF bemærker, at hvis omkostningerne tilvejebringes via gebyrfinansiering, vil virksomheder, der er omfattet af NIS-rammen, pålægges en dobbeltbyrde. **LF** bemærker hertil, at en asymmetrisk finansiering og håndhævelse kan skævvride konkurrencen på det indre marked. **LF** bemærker i forlængelse heraf, at en uligevægtig pålægning af administrative bøder kan bidrage skævt til konkurrencesituation, hvilket især er vigtigt med en bøderamme på op til 2 % af den samlede globale årsomsætning i en virksomhed.

TeleIndustrien (TI) finder regeringens og KOMs fastholdte fokus på den digitale infrastrukturs samfundskritiske funktion, positivt, og deler de førnævntes vurdering af, at økonomisk genoprejsning som

følge af COVID-19 krisen, i høj grad afhænger af en velfungerende og sikker teleinfrastruktur.

TI bemærker, at der i direktivet er meget eksplicit krav om, at der skal føres tilsyn, og at der skal være stærke muligheder for anvendelse af sanktioner fra den kompetente myndighed. Der nævnes bl.a., at den kompetente myndighed skal have mulighed for: onsite/offsite audit med stikprøver, regelmæssige tilsyn, tilsyn baseret på risikovurderinger eller risikorelateret tilgængelig information, sikkerhedsscanninger m.m. **TI** appellerer til, at disse beføjelser anvendes med omtanke, samt at der vil være et fokus på, at der ikke sker en konkurrenceforvirring. Historisk har myndighederne på teleområdet ikke anvendt de sanktionsmuligheder, de har haft, men i stedet fokuseret på dialog og samarbejde, hvilket **TI** anbefaler, at lovgivningen fortsat vil give plads til.

Specifikke bemærkninger

Genstand og anvendelsesområde

Artikel 1-2) **KL** bemærker, at kommunerne er pålagt ved lov at risikovurdere på kommunale behandlingsaktiviteter. Muligheden for, at der lægges nye metoder og rapporteringsforpligtigelser fra centralt hold ned over kommunerne er stor, og vil betyde yderligere omkostninger til ressourcer og håndtering af formelle krav til nye centrale risikovurderinger og dobbelt rapportering.

Artikel 1-2) **TI** hilser det foreslåede anvendelsesområde velkomment, herunder forpligtelser om, at medlemsstaterne skal vedtage en national
cybersikkerhedsstrategi, om risikostyring og rapportering vedrørende cybersikkerhed samt vedrørende udveksling af cybersikkerhedsoplysninger, hvor **TI** ikke forudser væsentlige ændringer i forhold til dansk praksis på teleområdet.

Artikel 2) **DEIT** kan i forlængelse af proportionalitetsprincippet støtte afgrænsningen, hvor direktivet – med visse undtagelser – ikke finder anvendelse på enheder, der betragtes som mikrovirksomheder eller små virksomheder.

Nationale rammer for cybersikkerhed

Artikel 5-11) **TI** bemærker, at såfremt samlingspunktet for CSIRT-arbejdet skulle blive Center for Cybersikkerhed, ser **TI** gerne, at der grundlæggende sker en opdeling således, at den/de myndighed(er)

eller enhed(er), som skal facilitere videndeling, udveksling af oplysninger, risikostyring og rapportering om fx cybersikkerhedshændelser, ikke er den/de samme myndighed(er), som også skal føre tilsyn, audits m.m., og som kan udstede sanktioner.

Artikel 6) **DEIT** bemærker, at det i lyset af sikkerhedstruslernes grænseoverskridende karakter er relevant, at de nationale CSIRT'er samarbejder på tværs af grænser i CSIRT-netværket, og at lade ENISA udvikle og vedligeholde et europæisk sårbarhedsregister. I forbindelse med offentliggørelser om sårbarheder, er det dog afgørende, at der i videst muligt omfang tages hensyn til beskyttelse af oplysninger, der deles af de i berørte virksomheder, herunder i særlig grad oplysninger, der kan have betydning for virksomhedens konkurrencesituation.

Artikel 6) **TI** bemærker, at udviklingen og vedligehold af et europæisk sårbarhedsregister i regi af ENISA findesumiddelbart positiv.

Artikel 7) **DEIT** bemærker, at i forbindelse med vedtagelse af en national cybersikkerhedshændelses- og kriseberedskabsplan bør NIS2 sikre, at det i højst mulig grad er muligt at bygge videre på de værdifulde indsatser, der allerede er iværksat for de kritiske samfundssektorer.

Artikel 10) **DEIT** bemærker, at CSIRT'ere pålægges en række omfattende opgaver. **DEIT** konstaterer hertil, at det ikke begrundes, hvorfor denne opgave bør udføres af en offentlig aktør frem for private cybersikkerhedsvirksomheder.

Samarbejde

Artikel 12) **TI** finder kravet om et konkret arbejdsprogram for de foranstaltninger, der skal iværksættes for at nå mål og opgaver, i medfør af stk. 5, afgørende for fremdrift af en sådan tværnational samarbejdsgruppe.**TI** bemærker, for så vidt hvad angår de foreslåede bestemmelser om samarbejde, herunder om et europæisk netværk af cybersikkerhedsorganisationer, at disse synes at være et naturligt næste skridt og noget, som er naturligt koordineret af de nationale CSIRT'er.

Forpligtelser vedrørende risikostyring og rapportering i forbindelse med cybersikkerhed

Artikel 17-19) **DSB** bemærker at der med artiklerne stilles nye krav til virksomhederne om metoder, proces og kompetenceniveau på området. **DSB** bemærker, at det betyder, at eksisterende praksis skal æn-

dres, hvilket kan medføre yderligere omkostninger. For at opnå en gevinst ved en mere aktiv involvering af myndighederne på dette område kræver det, at der oparbejdes et vist kompetenceniveau inden for cybersikkerhedsrisici.

Artikel 17-23) **TI** bemærker, i medfør af de foreslåede forpligtelser vedrørende risikostyring og rapportering i forbindelse med cybersikkerhed,
at de foreslåede bestemmelser om, at ledelsesorganer i alle enheder, der er omfattet af anvendelsesområdet, skal godkende de risikohåndteringsforanstaltninger vedrørende cybersikkerhed, der træffes af de respektive enheder, og følge specifik cybersikkerhedsrelateret uddannelse, er proportionale og naturlige.

Artikel 18) **DEIT** bemærker, at medlemsstaterne skal sikre, at de berørte enheder foretager en lang række omfattende foranstaltninger (jf. stk. 2). Kommissionen kan vedtage gennemførelsesretsakter med henblik på at fastlægge de tekniske og metodiske specifikationer for de i stk. 2 omhandlede elementer og tillægges beføjelser til at vedtage delegerede retsakter med henblik på at supplere de elementer, der er fastsat i stk. 2, for at tage hensyn til nye cybertrusler, den teknologiske udvikling eller sektor-specifikke særtræk. **DEIT** bemærker, at det nærmere bør præciseres, hvad det er for tekniske og metodiske specifikationer, der kan vedtages ved gennemførelsesretsakter, og **DEIT** bemærker i forlængelse heraf, at beføjelsen til at supplere elementerne, der er fastsat i stk. 2 forekommer temmelig bred, hvorfor **DEIT** ønsker en nærmere præcisering og begrænsning af beføjelsen.

Artikel 20) **DEIT** bemærker, at der er vigtigt, at indrapporterende enheder ikke risikerer, at der deles oplysninger, der kan skade virksomhedens konkurrenceposition. Det er væsentligt for at sikre virksomhedernes muligheder og fortsatte tillid i forbindelse med deling af oplysninger om sikkerhedshændelser. **DEIT** understreger, at stk. 6, omhandlende, at de myndighederne skal tage vare på den digitale tjenesteudbyders sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger, er yderst vigtig for virksomhederne. **DEIT** bemærker, at såfremt en kompetent myndighed eller CSIRT kræver, at offentligheden bliver informeret om en hændelse, bør deling af konkrete informationer ske i tæt konsultation med den berørte enhed for at forhindre deling af forretningskritiske oplysninger.

Artikel 20) **DSB** bemærker, at definitionen af hændelser inkluderer kommercielle tab og, at der efter **DSB**'s vurdering ikke er gradueret i forhold til væsentlighed. **DSB** foreslår, at "væsentlige" økonomiske tab tilføjes i artikel 20.

DSB bemærker videre, at hændelsesinformation skal tilgå CSIRT uden unødig forsinkelse, og senest 24 timer efter at virksomheden har fået kendskab til denne. **DSB** anfører, at håndteringen af cyberhændelser kræver særlige kompetencer og ressourcer, og at det er **DSB**'s forståelse, at kravet indebærer, at **DSB** etablerer et 24/7 stående beredskab. **DSB** bemærker, at en sådan udvidelse vil betyde en væsentlig omkostning for **DSB** i forhold til det eksisterende niveau. **DSB** finder i den forbindelse positivt, at medlemsstaterne fastsætter bestemmelser om, at den pågældende enhed i behørigt begrundede tilfælde og efter aftale med de kompetente myndigheder eller CSIRT'en kan fravige de fastsatte frister.

Artikel 20) **DANVA** bemærker, at fristerne for, hvornår hændelser skal afrapporteres, bør genovervejes. Fx om fristen for rapporter efter en måned er praktisk mulig og fornuftig.

Artikel 20) **DI** opfordrer til, at rapporteringsforpligtelserne sker med et minimum af administrative byrder for virksomhederne, der i forvejen pålægges at indrapportere på andre områder som f. eks. i regi af GDPR. Videreudvikling af den fælles indberetningsløsning som oprindeligt tænkt, så en enkelt virksomhedsindberetning dækker flere indrapporteringskrav og opfordringer, vil være positivt. Samtidig bør den nationale implementering sikre, at virksomhedernes både frivillige og påkrævede indrapportering automatisk undtages aktindsigt, som det allerede er indført i visse tilfælde ved indberetninger til Center for Cybersikkerhed. Endelig ser **DI** det som naturligt, at der også indføjes et krav til myndighederne om rapportering af viden tilbage til virksomhederne.

Artikel 21) **DSB** bemærker, at der introduceres yderligere certificeringsordninger/attester inden for cybersikkerhed. **DSB** foreslår, at nye ordninger ses i kontekst af allerede eksisterende foranstaltninger og kontrolmekanismer, så effekten optimeres i forhold til de ekstra omkostninger, der pålægges virksomheden.

Artikel 21) **TI** bemærker, at det er såvel positivt som proportionalt, at det er leverandøren, der skal sikre, at sikkerheden er på plads gennem en IKT-certificeringsordning. **TI** anbefaler, at der arbejdes for fælles standarder på tværs af EU's medlemslande.

Artikel 21) **DI** bemærker, at der i Danmark i 2021 lanceres en mærkningsordning for it-sikkerhed og ansvarlig data-anvendelse – d-mærket - der fra starten er tænkt til at bidrage til en europæisk mærknings-ordning baseret på de danske erfaringer. Regeringen bør opfordre Kommissionen til at se i den danske mærkningsordnings retning i forhold til at anbefale en passende europæisk mærkningsordning, der

kan understøtte, at en virksomhed lever op til direktivets forplig-telser om et passende cybersikkerhedsniveau.

Artikel 21) **DI** bemærker, at det danske mærkningsordningsprojekt, som **DI** er en af parterne bag, vil etablere en mærkningsordning for tillid til dataanvendelse, der både handler om it-sikkerhed, persondatabeskyttelse og om anvendelse af ny teknologi som kunstig intelligens. **DI** finder, at der ikke skal etableres flere mærkningsordninger for tillid til dataanvendelsen med hvert sit forskellige fokus; it-sikkerhed, privatlivsbeskyttelse, kunstig intelligens, Internet of Things osv, samt at førnævnte er en selvstændig pointe i lyset af, at Kommissionen også taler om mærkningsordningen på andre digitale områder.

Udveksling af oplysninger

Artikel 26-27) **TI** bemærker overordnet, at der ses en udfordring i at sikre vidensdeling, hvis samme myndighed eller enhed samtidig skal føre tilsynet. **TI** ønsker i denne sammenhæng, at videndelingen skal foregå i begge retninger: myndigheder skal pålægges at dele viden med aktørerne på samme måde, som aktørerne skal dele viden med myndighederne.

Artikel 26) **DSB** bemærker, at det fremgår, at virksomheder kan udveksle relevante cybersikkerhedsoplysninger. **DSB** bemærker, at der kan være tale om yderst forretningskritiske oplysninger, hvorfor **DSB** opfordrer til, at der lægges stor vægt på fortrolighed, herunder at der kun indsamles absolut nødvendig information.

Artikel 27) **TI** bemærker, at der er behov for klart at definere, hvad der karakteriseres som en "væsentlig hændelse" på europæisk niveau.

Tilsyn og håndhævelse

Artikel 28) **TI** bemærker, at henvisningen til fælles standarder på sårbarhedshåndteringsområdet, herunder håndhævelse af artikel 18, 20 og 22, af **TI** findes væsentlig for at sikre samordnet praksis. Hvis dette tilstræbes, bør disse fælles standarder, når de er kendt og vedtaget, ligeledes implementeres i dansk retstilling i form af udmøntning i bekendtgørelsen.

Artikel 29-30) **TI** bemærker umiddelbart forundring over skellet mellem "væsentlige enheder" og "vigtige enheder", i medfør af tilsyn og håndhævelse af sådanne.

Artikel 29-30) **DI** opfordrer til, at der samarbejdes med leverandører indenfor it-sikkerhed, og at markedet dermed inddrages i implementeringen af kontrol og tilsyns-regimet, så virksomheder bl.a. i videst mulig udstrækning kan anvende deres eksisterende it-sikkerhedsleverandør, som de har tillid til, til f.eks. sikkerhedsscanninger og anden kontrol og dokumentation.

Artikel 28-33) **DSB** bemærker, at der er tale om skærpede og udvidede beføjelser for medlemslandenes tilsyn og håndhævelse. **DSB** foreslår, at nye ordninger ses i kontekst af allerede eksisterende foranstaltninger og kontrolmekanismer, så effekten optimeres i forhold til de ekstra omkostninger, der pålægges virksomheden. **DSB** bemærker yderligere, at der foreslås udvidede muligheder for at pålægge bøder samt andre sanktioner. **DSB** bemærker hertil, at det kan skabe konkurrencefordele mellem virksomheder (f.eks. offentlige contra private virksomheder eller mellem virksomheder i forskellige lande).

Artikel 29-31) **KL** bemærker, at bøder ikke er hensigtsmæssige i forhold til offentlige myndigheder, herunder landets kommuner, og, at de øvrige foranstaltninger både vil være tilstrækkelige og langt mere effektive. KL bemærker i forlængelse heraf, at en kommune skal skære i den service, som kommunen leverer, på fx skoler eller i ældreplejen, hvis en kommune pålægges en meget stor bøde.

Artikel 31) **DEIT** bemærker, at overtrædelser af forpligtelserne i artikel 18 eller artikel 20 er administrative bøder på maksimalt mindst 10 mio. EUR eller op til 2 pct. af den samlede globale årsomsætning i den virksomhed, som den væsentlige eller vigtige enhed tilhører i det foregående regnskabsår, alt efter hvad der er højest. **DEIT** bemærker hertil, at bødeniveauet er meget højt samt, at berørte virksomheder ofte vil lide et økonomisk tab som følge af fx driftsforstyrrelser, manglende mulighed for afsætning eller tab af omdømme. I det lys konstaterer **DEIT**, at bødeniveauet på op til 10 mio. EUR eller 2 pct. af årsomsætningen forekommer ude af proportion.

Artikel 31) **DRFR** bemærker ift. administrative bøder, at det foreslåede niveau er fuldstændigt uacceptabelt. **DRFR** bemærker hertil, at en administrativ bøde vil være en dobbeltstraf for en virksomhed som er blevet udsat for en kriminel handling i form af et cyberangreb. **DRFR** bemærker, at en bøde sandsynligvis ikke vil være motiverende for deling af information og viden om et potentielt cyberangreb.

Øvrigt

Betragtning 38) **DS** foreslår, – på baggrund af betragtning 28, hvor internationale standarder bruges til at give et eksempel, hvor der kan

findes vejledninger til at opnå formålet med direktivet – at der henvises direkte til standarden ISO/IEC 27005, da denne giver en internationalt anerkendt vejledning til styring af "risiko". **DS** bemærker, at henvisningen til vejledningen vil give et fælles udgangspunkt for en definition på tværs af medlemslandene.

Betragtning 40) **DS** foreslår, – på baggrund af betragtning 28, hvor internationale standarder bruges til at give et eksempel, hvor der kan findes vejledninger til at opnå formålet med direktivet – at der henvises direkte til standarden ISO/IEC 27002, da denne giver en internationalt anerkendt vejledning til relevante informationssikkerhedsforanstaltninger. **DS** bemærker, at henvisningen til vejledningen vil give et fælles udgangspunkt for en definition på tværs af medlemslandene.

Bilag 7) **DSB** bemærker, de af Kommissionen anslåede udgiftsstigninger til overholdelses- og håndhævelsesaktiviteter. DSB bemærker, at ud fra erfaringer fra andre sektorer vil et øget kontrolpres fra myndighederne resultere i en øget omkostningsbyrde hos virksomhederne til at besvare og håndtere disse kontrolaktiviteter.

9. Generelle forventninger til andre landes holdninger

Der foreligger på nuværende tidspunkt ikke konkrete oplysninger om andre landes holdninger til forslaget.

10. Regeringens generelle holdning

Cybertruslen er en alvorlig trussel mod EU og Danmark. Regeringen ser med dyb alvor på, hvordan cyberangreb rammer virksomheder, myndigheder og demokratier med økonomiske og politiske konsekvenser til følge. Regeringen anerkender, at udviklingen i cybertruslerne sammenholdt med vores udbyggede digitale infrastruktur betyder, at cyberangreb har gode forudsætninger for at sprede sig i og på tværs af sektorer. I Danmark er truslen fra både cyberkriminalitet og cyberspionage meget høj. Derfor er cybersikkerhed en høj prioritet for regeringen.

Regeringen hilser på den baggrund Kommissionens forslag velkommen og ser positivt på ønsket om at højne cybersikkerheden og trusselsbevidstheden - også i yderligere sektorer, der ikke traditionelt arbejder med sikkerhed.

Regeringen arbejder generelt for at styrke samfundets resiliens, og forslaget flugter i høj grad med regeringens syn på beskyttelse af kritisk infrastruktur. Regeringen er enig i, at forslaget styrker modstandsdygtigheden ved at bidrage til et mere komplet og opdateret situationsbillede. Regeringen støtter i forlængelse heraf fokus på øget

samarbejde og vidensdeling, herunder udviklingen af et europæisk sårbarhedsregister.

Regeringen finder det samtidig meget vigtigt, at NIS-direktivet ikke medfører uforholdsmæssige eller unødige økonomiske byrder for aktører, som fra dansk side ikke er samfundsmæssigt eller økonomisk vigtige eller direkte afhængige af net- og informationssystemer, og at der tages hensyn til allerede eksisterende regulering og krav i sektorerne.

Regeringen finder det således meget vigtigt, at Danmark i lighed med det nuværende NIS-direktiv kan implementere NIS2 efter sektoransvarsprincippet.

Regeringen finder det meget vigtigt, at en eventuel udvidelse af NIS-direktivets dækningsområde i bredden og dybden sker med udgangspunkt i en risikobaseret tilgang, der sikrer proportionalitet i forhold til de cybersikkerhedskrav, som stilles i direktivet. Regeringen vil arbejde for at begrænse unødige administrative byrder. Regeringens endelige stillingtagen afventer en nærmere vurdering af de statslige og erhvervsøkonomiske konsekvenser.

Regeringen er som udgangspunkt positiv over for, at forslaget medfører en betydelig harmonisering på tværs af EU mht. hvilke virksomheder, der er omfattet af direktivet. Imidlertid indebærer forslagets lave grænse for, hvilke virksomheder der er omfattet, en risiko for at virksomheder, som ikke er samfundsmæssigt eller økonomisk vigtige, kan blive omfattet. Regeringen vil derfor arbejde for en mere målrettet og risikobaseret regulering.

Det er ikke klart for Regeringen, hvad der specifikt ligger i forslagets bestemmelser om gennemførselsretsakter, og regeringen ser et behov for præcisering og afgrænsning af bestemmelserne.

Der arbejdes i øjeblikket på at udforme en ny national strategi for cyber- og informationssikkerhed til afløsning af den gældende, som udløber i 2021. En ny strategi forventes at træde i kraft før et nyt NIS-direktiv er færdigforhandlet og skal implementeres i dansk lovgivning. Regeringen vil naturligvis bestræbe sig på overensstemmelse med dækningsområde og krav i den nationale strategi og de forventede krav som følger af et nyt NIS-direktiv.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Folketingets Europaudvalg blev orienteret d. 29. april 2021.