Ministeriet for Samfundssikkerhed og Beredskab

Dato: 6. februar 2025
Kontor: Sikkerhed

KOMMENTERET OVERSIGT
over
høringssvar om forslag til lov om foranstaltninger til sikring af højt cybersikkerhedsniveau
(NIS 2-loven)

Indhold

1. Høringen

1.1. Høringsperiode

Et udkast til lovforslag udarbejdet af Forsvarsministeriet har i perioden fra den 5. juli 2024 til den 22. august 2024 (48 dage) været sendt i høring hos en række myndigheder, organisationer m.v.

Udkastet til lovforslag blev den 5. juli 2024 sendt til Folketingets Forsvarsudvalg og Udvalg for Digitalisering og It til orientering, og blev samtidig offentliggjort på Høringsportalen den 5. juli 2024.

Med den kongelige resolution af 29. august 2024 har Ministeriet for Samfundssikkerhed og Beredskab overtaget det overordnede ansvar for implementeringen af direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele EU (NIS 2-direktivet) fra Forsvarsministeriet.

1.2. Hørte myndigheder og organisationer mv.

Nedenfor følger en alfabetisk oversigt over hørte myndigheder og organisationer mv.

Ud for hver høringspart er det ved afkrydsning angivet, om der er modtaget høringssvar, og om høringsparten i givet fald har haft bemærkninger til udkastet til lovforslag.

Oversigten omfatter herudover interessenter, som ikke er blandt de hørte myndigheder, organisationer mv., men på egen foranledning har sendt bemærkninger til udkastet til lovforslag. Sådanne interessenter er i oversigten markeret med *.

Høringspart	**Høringssvar modtaget**	**Bemærkninger**	**Ingen bemærkninger**
Advokatrådet	x	x	
Amnesty International			
ATP	x	x	
Bestyrelsesforeningen			
Biogas Danmark	x	x	
Danish Care			
Danish Cloud Community			
Danish Seafood Association			
Danmarks Apotekerforening	x	x	
Dansk Arbejdsgiverforening			
Dansk Erhverv	x	x	
Dansk Industri	x	x	
Dansk IT			
Dansk Kollektiv Trafik			
Dansk Luftfart			
Dansk Selskab for Patientsikkerhed			
Dansk Standard	x	x	
Danske Advokater			
Danske Havne	x	x	
Danske Maritime			
Danske Rederier	x	x	
Danske Regioner	x	x	
Danske Shipping- og Havnevirksomheder			

Danske Universiteter	x	x	
Danske Vandværker	x	x	
DANVA	x	x	
Dataetisk Råd			
Datatilsynet	x	x	
Danish e-infrastructure consortium	x	x	
De Samvirkende Købmænd	x	x	
Den Danske Dommerforening			
Den Danske Søretsforening			
Dansk Internet Forum (DIFO)	x	x	
DJØF			
DKCERT	x	x	
D-mærket	x	x	
Digitaliseringsstyrelsen i Grønland	x	x	
Domstolsstyrelsen		x	
DSB	x	x	
Erhvervsflyvningens sammenslutning	x	x	
Fagbevægelsens Hovedorganisation			
Finans Danmark			
Forenede Danske Antenneanlæg	x	x	
FSR – Danske Revisorer*	x	x	
Færgerederierne*	x	x	
Færøernes Landsstyre via Rigsombudsmanden på Færøerne	x	x	
Green Power Denmark	x	x	
GTS-foreningen	x	x	
Ingeniørforeningen i Danmark	x	x	
Industriens Fond	x	x	

Industriforeningen for Generiske og Biosimilære Lægemidler			
Institut for Menneskerettigheder			
IT-Branchen	x	x	
International Transport Danmark	x	x	
IT-politisk forening			
IT-Universitetet			
John Michael Foley	x	x	
Justitia			
KOMBIT	x	x	
Kommunale Velfærdschefer	x		x
Kommunernes Landsforening	x	x	
Københavns Byret			
Københavns Lufthavne	x	x	
Landbrug og Fødevarer	x	x	
Lederne			
Lægemiddelindustriforeningen			
MEDCOM			
Medicoindustrien	x	x	
NaviAir*	x		x
NORDUnet A/S			
Pharmadanmark			
Præsidenten for Vestre Landsret			
Præsidenten for Østre Landsret			
Punktum dk	x		
Retspolitisk Forening			
Rigsrevisionen	x		x
Rådet for Digital Sikkerhed	x	x	
SamAqua	x	x	

Samtlige byretspræsidenter			
Tekniq Arbejdsgiverne	x	x	
Teleindustrien*	x	x	
Trafikselskaberne i Danmark	x		

2. Høringssvarene

Nedenfor er gengivet de væsentligste punkter i de modtagne høringssvar. Ministeriet for Samfundssikkerhed og Beredskabs bemærkninger til høringssvarene, herunder om der er foretaget ændringer i anledning af høringssvarene, er skrevet med kursiv.

Under pkt. 3 er det opsummeret, hvilke ændringer der er foretaget i forhold til det udkast, som har været i offentlig høring.

Samtlige høringssvar er vedlagt særskilt.

2.1. Generelle bemærkninger til lovforslaget

Danske Universiteter og Danske Rederier anerkender vigtigheden af, at implementeringen af NIS 2-direkivet kan være med til at styrke Danmarks sikkerhed mod cybertrusler.

Dansk Erhverv bemærker, at det i lyset af det forhøjede trusselsniveau mod danske virksomheder fra cyberangreb som følge af den geopolitiske situation i Europa, af øget digitalisering og øget tilgængelighed af cybervåben er meget positivt, at reguleringen omkring virksomhedernes beredskab nu styrkes.

Danske Universiteter bemærker, at universitetssektoren er meget bevidst om det øgede trusselsniveau, der er på sektoren, og anser arbejdet med cyber- og informationssikkerhed som en grundlæggende forudsætning for, at universiteterne kan understøtte forskning og uddannelse.

Dansk Erhverv, Danske Regioner og Danske Universiteter bakker op om lovforslagets risikobaserede tilgang, og fremhæver, at den

risikobaserede tilgang bør fastholdes gennem hele implementeringen af NIS 2-direktivet.

Ministeriet for Samfundssikkerhed og Beredskab noterer sig synspunkterne.

Advokatsamfundet, IT-Branchen, Industriens Fond, IDA, DANVA, Danske Universiteter, Dansk Industri (DI), Dansk Erhverv, TEKNIQ Arbejdsgiverne, Rådet for Digital Sikkerhed og Medico Industrien understreger behovet for vejledningsmateriale, som supplerer lovens definitioner og krav, herunder bl.a. vedrørende foranstaltninger og hændelsesindberetninger.

Ministeriet for Samfundssikkerhed og Beredskab kan oplyse, at der vil blive udarbejdet vejledningsmateriale vedrørende bl.a. lovens anvendelsesområde og krav til foranstaltninger, som vil foreligge senest ved lovens ikrafttræden. Hertil kommer, at de kompetente myndigheder i relevant omfang vil yde vejledning til enheder, der er omfattet af lovens anvendelsesområde.

Advokatrådet, Landbrug og Fødevarer, International Transport Danmark (ITD), Danske Rederier, Danske Universiteter, Danske Regioner, Dansk Industri og Medico Industrien finder det positivt, at der med lovforslaget tages udgangspunkt i en minimumsimplementering.

Advokatrådet og DANVA noterer, at minimumsimplementeringen ikke bør stå i vejen for, at loven bliver operationel og smidig, og at sektorspecifikke bekendtgørelser ikke blot bør gentage indholdet af lovbestemmelserne.

Ministeriet for Samfundssikkerhed og Beredskab noterer sig synspunkterne.

Digitaliseringsstyrelsen i Grønland bemærker, at Grønlands Selvstyre har til hensigt at etablere en kompetent myndighed med de samme formål, som lovforslaget har for kompetente myndigheder i

Danmark. Digitaliseringsstyrelsen i Grønland bemærker endvidere, at Grønlands Selvstyre har en stærk interesse i at kunne deltage i et samarbejde, hvor en grønlandsk kompetent myndighed kan blive involveret i en væsentlig hændelse, der måtte ske i kritiske it-systemer, der vil kunne have virkning i Grønland.

Ministeriet for Samfundssikkerhed og Beredskab noterer sig Digitaliseringsstyrelsen i Grønlands bemærkninger og vil gå i dialog med styrelsen herom.

2.2. Bemærkninger til de enkelte punkter i lovforslaget
2.2.1. Lovens anvendelsesområde
2.2.1.1. Vurdering af, hvorvidt en enhed er omfattet af lovens anvendelsesområde

Advokatsamfundet, IT-branchen, International Transport Danmark, SamAqua, Dansk Industri og Dansk Erhverv finder, at virksomheder bør kunne rette henvendelse til en sektoransvarlig myndighed og modtage en afgørelse eller bindende svar på, om de er omfattede af NIS 2 eller ej.

Danske Regioner, TEKNIQ Arbejdsgiverne, Rådet for Digital Sikkerhed, SamAqua, Dansk Industri, og Dansk Erhverv efterlyser præcisering af, hvilke virksomheder der reelt er omfattet, herunder en afklaring af, hvorvidt en virksomhed og koncernforbundne selskaber er omfattet eller ej.

Danmarks Apotekerforening, ATP, Trafikselskaberne i Danmark, Danske vandværker, Biogas Danmark, Forenede Danske Antenneanlæg, International Transport Danmark, SamAqua, Danske Universiteter og Domstolsstyrelsen sætter spørgsmålstegn ved forståelsen af anvendelsesområdet, herunder om de eller deres medlemmer er omfattet heraf og foreslår, at spørgsmålet afklares i loven eller dennes bemærkninger.

Danske Rederier har bemærket, at det af lovbemærkningerne fremgår, at hele enheden anses for omfattet af direktivets anvendelsesområde, også selv om enheden har flere forretningsområder eller er opdelt

i flere administrative enheder, og det eksempelvis alene er ét af disse forretningsområder, som er omfattet af de sektorer, der er omhandlet i direktivets bilag. Der efterlyses en nærmere afklaring af, hvilken betydning denne tilgang vil have for, at en enhed bliver omfattet af reguleringen i relation til kriterierne for mellemstore og store virksomheder (antal beskæftigede og finansielle tærskler).

Dansk Erhverv peger på, at der er usikkerhed og forskellige meldinger i sektorerne om de størrelseskrav, der stilles til omfattede enheder.

Medicoindustrien bemærker, at det er positivt, at det af bemærkningerne til lovforslaget fremgår, at en relevant kompetent myndighed kan træffe afgørelse om, at en enhed, der som udgangspunkt anses for at være væsentlig, i stedet skal anses for at være vigtig.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at den ordning, der følger af lovforslaget, vil indebære, at de enkelte enheder på baggrund af en vurdering af, hvorvidt enheden er er omfattet af de omfattede sektorer og om enheden opfylder størrelseskravet, skal tage stilling til, om enheden er omfattet af lovforslaget.

Det bemærkes, at der i tilknytning til loven vil blive udarbejdet vejledninger, der bl.a. vil belyse lovens anvendelsesområde. Hertil kommer, at de kompetente myndigheder i relevant omfang vil yde vejledning til enheder, herunder om, hvorvidt enheden er omfattet af lovens anvendelsesområde. Vejledningerne vil foreligge senest ved lovens ikrafttræden.

Ministeriet for Samfundssikkerhed og Beredskab kan endvidere oplyse, at ministeriet har justeret bemærkningerne til lovforslaget med henblik på, at det fremtræder klarere, hvilke virksomheder og koncernforbundne selskaber, der opfylder de stillede krav til antal beskæftigede og til virksomhedens økonomi.

Samtidig har Ministeriet for Samfundssikkerhed og Beredskab tydeliggjort i lovforslaget, hvilke offentlige forvaltningsmyndigheder, der er omfattet af loven.
For så vidt angår spørgsmålet om, hvorvidt hele enheden anses for omfattet af lovens anvendelsesområde, har Ministeriet for

Samfundssikkerhed og Beredskab foretaget tilpasninger i lovforslaget, navnlig i lyset i lyset af EU-Kommissionens meddelelse C(2023) 6068 af 13. september 2023 om retningslinjer for anvendelsen af artikel 4, stk. 1, og 2, i NIS 2-direktivet. Det er på den baggrund Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at formuleringen »i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester« i NIS 2-direktivets artikel 21, stk. 1, skal forstås som alle de net- og informationssystemer, som disse enheder anvender til deres operationer, eller til at levere deres tjenester, og ikke kun specifikke informationsteknologiske (it) aktiver eller kritiske tjenester, som enheden leverer.

I tilfælde, hvor en enhed anvender flere forskellige typer af net- og informationssystemer, og hvor kun nogle af disse systemer er omfattet af direktivets bilag, vil samtlige af de net- og informationssystemer, som enheden anvender til sine operationer, eller til at levere sine tjenester, således blive underlagt direktivets krav.

Der henvises i øvrigt til lovforslagets pkt. 3.1. og bemærkningerne til den foreslåede § 1.

2.2.1.2. Anvendelsesområde for kommuner

KL, IDA, IT-Branchen, KOMBIT, Rådet for Digital Sikkerhed og Dansk Erhverv understreger, at kommuner bør omfattes af lovens anvendelsesområde.

Ministeriet for Samfundssikkerhed og Beredskab har noteret sig synspunktet. Ministeriet bemærker, at det ifølge NIS 2-direktivet er op til medlemsstaterne, om direktivet skal finde anvendelse på offentlige forvaltningsenheder på lokalt plan, jf. den foreslåede § 1, stk. 6.

Det bemærkes, at en kommune efter omstændighederne kan være omfattet af lovens anvendelsesområde, selvom bemyndigelsen i det foreslåede § 1, stk. 6, ikke er udnyttet. Dette vil eksempelvis være tilfældet i en situation, hvor en kommune agerer som sundhedstjenesteyder i overensstemmelse med NIS 2-direktivets bilag I og II. I denne situation vil kommunen være omfattet af lovens anvendelsesområde på baggrund af disse aktiviteter, også selvom bemyndigelsen i den foreslåede bestemmelse ikke er udnyttet.

Det er Ministeriet for Samfundssikkerheds opfattelse, at en kommune i sådanne tilfælde som helhed være omfattet af lovens krav. Der henvises i den forbindelse til lovforslagets pkt. 3.1.3, hvoraf det bl.a. fremgår, at i tilfælde, hvor en enhed leverer flere forskellige typer af net- og informationssystemer, og hvor kun nogle af disse systemer er omfattet af direktivets bilag, vil samtlige af de net- og informationssystemer, som enheden anvender til sine operationer, eller til at levere sine tjenester, således blive underlagt direktivets krav.
Ministeriet for Samfundssikkerhed har på den baggrund præciseret i lovforslaget, at bl.a. kommuner ikke alene vil skulle træffe passende og forholdsmæssige foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer vedrørende de aktiviteter, der er oplistet i direktivets bilag, men for samtlige af de net- og informationssystemer, som de anvender til deres operationer, eller til at levere deres tjenester.

Den foreslåede bestemmelse i stk. 6 vil således alene være relevant, hvis man måtte ønske at omfatte offentlige forvaltningsenheder på lokalt plan eller uddannelsesinstitutioner, der ikke allerede er omfattet af direktivets anvendelsesområde.

Der henvises til lovforslagets pkt. 3.1.3. og bemærkningerne til den foreslåede § 1, stk. 6.

KL og Dansk Erhverv finder, at det vil være uheldigt, hvis offentlig WIFI på biblioteket og i borgerservice vil være en teleydelse, der er omfattet af NIS 2, hvor kommunen sidestilles med en teleudbyder. Det vil medføre unødigt bureaukrati at tilbyde den service fremadrettet, og det kan lede til, at kommunerne stopper med at tilbyde dette.

Ministeriet for Sikkerhed og Beredskab bemærker, at NIS 2-loven som udgangspunkt ikke finder anvendelse for telesektoren, idet NIS 2-direktivet for telesektoren implementeres særskilt gennem forslag til lov om sikkerhed og beredskab i telesektoren. Det følger imidlertid af den foreslåede § 1, stk. 1, i forslag til lov om sikkerhed og beredskab i telesektoren, at denne lov ikke finder anvendelse for kommuner og

regioner, der stiller offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester til rådighed, idet sådanne kommuner og regioner omfattes af forslag til NIS 2-loven.

For at sikre ensartethed mellem den foreslåede NIS 2-lov og forslag til lov om sikkerhed og beredskab i telesektoren for så vidt angår definitionen af en teleudbyder, har Ministeriet for Samfundssikkerhed og beredskab justeret den foreslåede § 4, stk. 2, således at kommuner og regioner alene vil anses som teleudbydere i det omfang de med et kommercielt formål måtte udføre opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester. Dertil skal kommunen eller regionen opfylde størrelseskravet i den foreslåede § 4, stk. 2, nr. 1 og 2.

Der henvises til bemærkningerne til den foreslåede § 4, st. 2.

2.2.1.3. Afgrænsningen af væsentlige og vigtige enheder
Dansk Industri anfører, at afgrænsningen af væsentlige enheder efter de kvalitative kriterier i lovforslagets § 4, stk. 3, nr. 5, bør ske ud fra en risikobaseret tilgang og i tæt dialog med de pågældende virksomheder.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at stillingtagen til, om en enhed er omfattet af bestemmelsen eller ej, skal afgøres på baggrund af en konkret og individuel vurdering.

Det bemærkes, at bestemmelsen har et forholdsvist skønsmæssigt og kvalitativt præg, hvilket kan gøre det vanskeligt for de enkelte enheder at vurdere, om de er omfattet af lovens krav til henholdsvis væsentlige eller vigtige enheder. Det forudsættes derfor, at de kompetente myndigheder i relevant omfang vejleder enheder inden for deres sektor om forståelsen af § 4, stk. 3, nr. 5.

Der vil derudover blive udarbejdet vejledningsmateriale, som vil foreligge senest samtidig med lovforslagets ikrafttræden, der vil hjælpe

enheder med at vurdere, om de er omfattet af den foreslåede § 4, stk. 3, nr. 5.

Det bemærkes derudover, at den foreslåede § 4, stk. 4, bemyndiger vedkommende minister til efter forhandling med ministeren for samfundssikkerhed og beredskab at fastsætte nærmere regler om kriteriet for, hvornår enheder er omfattet af den foreslåede § 4, stk. 3, nr. 5.

De kompetente myndigheder vil med den foreslåede bestemmelse kunne uddybe de skønsmæssige kriterier i bestemmelsens stk. 3, nr. 5, således at kriterierne tilpasses særlige sektorspecifikke forhold. De kompetente myndigheder vil eksempelvis kunne fastsætte nærmere regler om, hvornår en forstyrrelse af den tjeneste, som enheder leverer inden for sin sektor, vil kunne medføre en væsentlig systemisk risiko.

Derudover vil enheder i overensstemmelse med forvaltningslovens § 7 i fornødent omfang kunne få vejledning og bistand fra de kompetente myndigheder.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 4, stk. 3, nr. 5.

2.2.2. Foranstaltninger til styring af cybersikkerhedsrisici
2.2.2.1. Anvendelse af standarder
Dansk Industri bemærker, at standarder bidrager til at sikre en ensrettet tilgang på tværs af medlemsstaterne og kan styrke det generelle cybersikkerhedsniveau på tværs, og at NIS 2-direktivets artikel 21 og artikel 25 bør afspejles i lovforslaget ved indsættelse af en bestemmelse herom.

D-mærket, Dansk Industri og Erhvervsflyvningens Sammenslutning finder sammenfattende, at europæiske eller internationalt accepterede sikkerhedsstandarder eller EU-landenes egne nationale standarder som anvendes af omfattede enheder, bør kunne anvendes som dokumentation for, at enheder efterlever direktivets krav om foranstaltninger.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at NIS 2-direktivets artikel 21, stk. 1 og artikel 25, stk. 1, skal forstås således, at relevante internationale standarder kan benyttes som led i opfyldelse af direktivets krav om foranstaltninger, men at en enhed ikke kan anses for at opfylder direktivets krav alene ved at være eksempelvis ISO-certificeret.

På denne baggrund har Ministeriet for Samfundssikkerhed og Beredskab skrevet frem i lovforslaget, at relevante europæiske og internationale standarder som for eksempel ISO/IEC 27000-serien, IEC 62443-standarder, NIST-standarder og ETSI TR 103 305-standarder kan anvendes som et rammeværktøj til at træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 6.

2.2.2.2. Forsyningskædesikkerhed og forholdet til underleverandører
Dansk Industri, Danske Rederier, Advokatsamfundet, ATP og D-mærket har bl.a. anført, at der som følge af uklarhed omkring krav til underleverandører er risiko for, at direkte omfattede virksomheder vil skubbe alle krav ned i leverandørkæden for at sikre overholdelse. Dette kan medføre uforholdsmæssigt store byrder for leverandører, og der bør sikres en risikobaseret tilgang og vejledning omkring, i hvilket omfang leverandørers leverancer også er omfattet.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at det fremgår af NIS 2-direktivets præambelbetragtning nr. 85 , at håndtering af risici, der stammer fra en enheds forsyningskæde og dens forhold til sine leverandører såsom udbydere af datalagrings- og databehandlingstjenester eller udbydere af administrerede sikkerhedstjenester og softwareudgivere, er særlig vigtig i betragtning af udbredelsen af hændelser, hvor enheder har været udsat for cyberangreb, og hvor ondsindede gerningspersoner har været i stand til at kompromittere sikkerheden af en enheds net- og informationssystemer ved at udnytte sårbarheder, der påvirker tredjepartsprodukter og -tjenester. Væsentlige og vigtige enheder bør derfor vurdere og tage hensyn til den generelle kvalitet og modstandsdygtighed af produkter og

tjenester, de heri integrerede foranstaltninger til styring af cybersikkerhedsrisici og deres leverandørers og tjenesteudbyderes cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Væsentlige og vigtige enheder bør navnlig tilskyndes til at indarbejde foranstaltninger til styring af cybersikkerhedsrisici i kontraktlige arrangementer med deres direkte leverandører og tjenesteudbydere.

På den baggrund er væsentlige og vigtige enheder efter lovforslagets § 6 forpligtet til at træffe foranstaltninger, der som minimum omfatter eller tager højde for bl.a., forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.

Dette betyder, at væsentlige og vigtige enheder er ansvarlige for, at deres foranstaltninger til styring af cybersikkerheden omfatter eller tager højde for forsyningssikkerhed som nævnt ovenfor. Dette vil f.eks. kunne ske ved, at enheden stiller krav til sine underleverandører om, at disse opfylder bestemte krav og forpligtelser, eller at enheden fastsætter procedurer mv. med henblik på at sikre, at enhedens underleverandørers produkter mv. ikke medfører cybersikkerhedsrisici hos den pågældende enhed.

Enhederne er alene ansvarlige for cybersikkerheden i enheden, men et element heri er naturligt at være opmærksom på, om enhedens eventuelle underleverandører kan udgøre en cybersikkerhedsrisiko, og hvordan dette kan afværges.

2.2.3. Definitionen af et ledelsesorgan

SamAqua, **DANVA, Green Power Denmark, Dansk Industri, Dansk Standard, Danske Rederier, ATP og DIFO** efterlyser en afklaring af, hvad der forstås ved en enheds ledelsesorgan, herunder hvem der er omfattet.

Lov om aktie- og anpartsselskaber, jf. lovbekendtgørelse nr. 1168 af 1. september 2023 (selskabsloven), definerer i § 5, nr. 4 'det centrale ledelsesorgan' som a) bestyrelsen i selskaber, der har en direktion og en bestyrelse, b) direktionen i selskaber, der alene har en direktion og c) direktionen i selskaber, der både har en direktion og et tilsynsråd.

Selskabsloven finder dog alene anvendelse for aktie- og anpartsselskaber, jf. lovens § 1, stk. 1.

Lov om visse erhvervsdrivende virksomheder, jf. lovbekendtgørelse nr. 249 af 1. februar 2021 (LEV-loven), definerer i lovens § 4 a, nr. 2, en ledelse, som 'medlemmer af bestyrelse, direktion eller et tilsvarende ledelsesorgan'.

LEV-loven finder anvendelse for enkeltmandsvirksomheder, interessentskaber, kommanditselskaber, andelsselskaber (andelsforeninger) samt andre selskaber og foreninger med begrænset ansvar, som ikke er omfattet af selskabsloven, lov om erhvervsdrivende fonde eller §§ 133-154 i lov om forvaltere af alternative investeringsfonde m.v., jf. LEV-lovens § 1, stk. 2.

Ministeriet for Samfundssikkerhed og Beredskab har bl.a. på baggrund af de indkomne høringssvar foretaget en præcisering af begrebet 'ledelsesorgan', således at der nu af de specielle bemærkninger til lovforslagets § 6 bl.a. fremgår, at begrebet 'ledelsesorgan' i NIS 2-direktivet skal forstås i overensstemmelse med definitionerne af henholdsvis det centrale ledelsesorgan i selskabslovens § 5, nr. 4, og ledelsen i LEV-lovens § 4 a, nr. 2.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 7, stk. 1 og lovforslagets pkt. 3.2.4.

2.2.4. Underretninger om væsentlige hændelser

Dansk Erhverv anfører, at en række af Dansk Erhvervs medlemmer efterspørger en afklaring om hændelsesrapportering for globale virksomheder.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at det fremgår af bemærkningerne til den forslåede bestemmelse i § 12 , at såfremt en væsentlig hændelse, der underrettes om, måtte have grænseoverskridende virkning, vil CSIRT'en i overensstemmelse med forudsætningen i NIS 2-direktivets artikel 23, stk. 6, via det centrale kontaktpunkt uden unødigt ophold skulle underrette de øvrige berørte medlemsstater og ENISA om den væsentlige hændelse, navnlig hvor den væsentlige hændelse berører to eller flere medlemsstater. Efter

samme bestemmelse vil en sådan information omfatte den type af oplysninger, der er modtaget i overensstemmelse med artikel 23, stk. 4, og CSIRT'en vil i den forbindelse – i overensstemmelse med EU-retten eller national ret – sikre enhedens sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 12.

2.2.5. Offentliggørelse

Dansk Industri har bl.a. anført, at det af § 16, stk.1, fremgår, at en sektoransvarlig myndighed, efter høring af virksomheden kan informere offentligheden om en væsentlig hændelse, mens myndigheden efter § 16, stk. 2, kan kræve, at virksomheden informerer offentligheden. Det er uklart, om der i situationer, hvor offentligheden bør informeres, er et delt ansvar mellem myndighed og virksomhed i forhold til at informere offentligheden.

ATP bemærker, at det i lovteksten bør præciseres, at der kan ske offentliggørelse, hvis denne er af væsentlig interesse for offentligheden. Dette vil sikre, at det EU-retlige proportionalitetsprincip, der gælder for fortolkningen af direktivet, også afspejles i den danske lovtekst.

IT-branchen anfører, at det i lovforslaget bør præciseres, hvornår/hvor hurtigt en hændelse kan offentliggøres, f.eks. om der vil være tilstrækkelig tid til, at den pågældende enhed kan have håndteret hændelsen, og hvor lang tid høringen af den pågældende enhed vil/kan være.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at den foreslåede § 16bestemmelsen implementerer NIS 2-direktivets artikel 23, stk. 7, hvoraf det fremgår, at hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed, og hvor det er relevant CSIRT'erne eller de kompetente myndigheder i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

Den kompetente myndighed kan således beslutte, om informering af offentligheden skal ske af myndigheden eller af den relevante enhed.

For så vidt angår proportionalitet i vurderingen af, om oplysninger om en hændelse skal offentliggøres, bemærker Ministeriet for Samfundssikkerhed og Beredskab, at den foreslåede bestemmelse i § 16, stk. 1, indebærer, at den relevante kompetente myndighed kan informere offentligheden om en væsentlig hændelse, hvis offentliggørelsen er nødvendig for at forebygge eller håndtere hændelsen, eller hvor offentliggørelsen af hændelsen på anden vis er i offentlighedens interesse.

Ministeriet bemærker videre, at den relevante kompetente myndighed i medfør af bestemmelsen vil skulle høre den berørte enhed, før der sker offentliggørelse af hændelsen. Formålet med høringen vil være at sikre, at den kompetente myndighed kan træffe afgørelse om offentliggørelse på et oplyst grundlag, herunder foretage en afvejning af hensynet til den konkrete enhed over for hensynet til orientering af offentligheden. Det vil i den forbindelse skulle sikres, at offentligheden informeres på en ansvarlig måde, som ikke kompromitterer fortrolige oplysninger.

For så vidt angår tidspunktet for offentliggørelse bemærkes, at den konkrete fastsættelse af en høringsfrist vil bero på en samlet afvejning, hvori også indgår hensynet til at vedkommende enhed har en rimelig tid til at afgive en udtalelse. Afhængig af karakteren af den væsentlige hændelse vil høringsfristen efter omstændighederne kunne være relativt kort.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 16.

2.2.6. Tilsyns- og håndhævelsesforanstaltninger

2.2.6.1. Tilsyn med væsentlige enheder

Advokatsamfundet og Dansk Erhverv anbefaler, at det behandles nærmere i lovforslaget, om et forbud mod at udøve ledelsesfunktioner kan meddeles en person, uden at den pågældende konkret har foretaget dadelværdige forhold eller forsømmelser (objektivt ansvar), eller om anvendelsen af et forbud forudsætter, at den pågældende konkret har været vidende om eller deltaget i beslutninger, der vedrører de forhold, som forbuddet søger at adressere.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at en kompetent myndigheds overvejelse og anvendelse af hjemmelen til midlertidigt at forbyde enhver person at udøve ledelsesfunktioner i den pågældende væsentlige enhed alene kan bringes i anvendelse i situationer, hvor de håndhævelsesforanstaltninger, der er pålagt i medfør af de foreslåede § 22, nr. 1-4, har vist sig at være utilstrækkelige, og hvor den kompetente myndighed herefter har fastsat en frist, inden for hvilke den væsentlige enhed skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde den kompetente myndigheds krav.

Som nærmere beskrevet i lovforslagets pkt. 5.3.2.2. vil et eventuelt strafansvar for fysiske personer følge det almindelige udgangspunkt i særlovgivningen. Der vil således kunne rejses tiltalt mod en fysisk person, såfremt denne har handlet forsætligt eller groft uagtsomt. Bøder vil i givet fald skulle udmåles i overensstemmelse med direktivets forudsætninger om størrelsen heraf.

2.2.6.2. Tilsyn med vigtigt enheder

Dansk Industri har bl.a. anført, at jf. § 24 forventes myndighederne at have en reaktiv tilgang til tilsyn over for vigtige enheder. Kriterierne for, hvornår dette tilsyn aktiveres, bør defineres tydeligere.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at det fremgår af bemærkningerne til bestemmelsen, at det reaktive tilsyn med vigtige enheder eksempelvis vil kunne aktiveres, hvis der modtages oplysninger fra andre myndigheder, enheder, borgere eller i medier, eller hvis myndigheden i forbindelse med udførelsen af dennes opgaver i øvrigt kommer i besiddelse af oplysninger, der peger på mulige overtrædelser af reguleringen.

Det fremgår videre af bemærkningerne, at et reaktivt tilsyn kan iværksættes på baggrund af oplysninger, der tyder på, at den pågældende enhed potentielt ikke efterlever sine forpligtelser efter loven og regler udstedt i medfør af loven, herunder eventuelt efter en væsentlig hændelse. Det reaktive tilsyn vil således kunne iværksættes på baggrund af oplysninger, som de kompetente myndigheder modtager fra andre myndigheder, enheder, borgere, medier eller andre kilder eller offentligt tilgængelige oplysninger. Det kan desuden eksempelvis være

oplysninger, der hidrører fra andre aktiviteter, der indgår i de kompetente myndigheders udførelse af deres arbejdsopgaver.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 24.

2.2.6.3. Koordinering mellem de kompetente myndigheder

Danske universiteter bemærker, at der for enheder som indgår i flere sektorer kan opstå udfordringer. Danske universiteter opfordrer derfor til at sikre en høj grad af koordinering mellem ressortmyndighederne.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at det i lovforslaget forudsættes, at der vil være en tæt koordination mellem de kompetente myndigheder i forbindelse med tilrettelæggelsen af tilsynsarbejdet, således at der i videst muligt omfang anlægges en fælles tilgang. Dette vil særligt være relevant for tilsynet med enheder, der måtte indgå i flere forskellige sektorer, og hvor der potentielt er flere kompetente myndigheder, som skal føre tilsyn med samme enhed.

Ministeriet for Samfundssikkerhed og Beredskab har på denne baggrund indsat en ny bemyndigelsesbestemmelse i lovforslagets § 20, stk. 3, der bemyndiger ministeren for samfundssikkerhed og beredskab til at fastsætte nærmere regler om koordinering, ansvar, fordeling af opgaver og udveksling af oplysninger mellem henholdsvis de kompetente myndigheder samt de kompetente myndigheder og CSIRT'en, herunder i forhold til hændelsesunderretninger efter kapitel 3, tilsyn samt håndhævelse efter kapitel 6.

Der henvises til bemærkningerne til den foreslåede § 20, stk. 3, og i øvrigt til lovforslagets pkt. 2.2.2.

2.2.7. Regler om digital kommunikation

Dansk Industri har bl.a. anført, at det bør sikres, at der til enhver tid er alternative kommunikationsveje, så hverken myndigheder eller virksomheder er afhængige af kun én digital løsning.

ATP har bemærket, at f.eks. i forbindelse med underretninger, vil disse skulle ske i forbindelse med hændelser, hvor det er sandsynligt, at enhedens digitale muligheder er kompromitterede. Ligeledes kan de

offentlige selvbetjeningsløsninger være nede, fx MitID eller lignende. Det kan derfor overvejes at give mulighed for indberetninger på anden vis, fx telefonisk, hvis det ikke er praktisk muligt at tilgå de offentlige løsninger.

IT-Branchen bemærker, at for at lette de administrative omkostninger for erhvervslivet og fremme den generelle indberetning, vil det være vigtigt, at der faciliteres én indberetning/indgang/formular – også for væsentlige og vigtige enheder, der er beskæftiget i mere end én af de NIS2- omfattede sektorer (à la Virk.dk i dag).

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at det fremgår af den foreslåede bestemmelse i § 31, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur eller lignende.

Ministeriet for Samfundssikkerhed og Beredskab har noteret sig bemærkningerne, og vil sørge for, at de indgår i det videre arbejde med udarbejdelse af bekendtgørelsen om digital kommunikation.

For så vidt angår indberetningsløsningen, fremgår det af lovforslagets pkt. 3.3.1, at underretninger om hændelser i dag indgives via selvbetjeningsløsningen Virk.dk. Når der indgives en hændelsesrapportering på Virk.dk, fordeles denne automatisk til den eller de relevante kompetente myndigheder, CSIRT'en og det centrale kontaktpunkt.

Ministeriet for Samfundssikkerhed og Beredskab forventer, at hændelsesunderretningen fremover på tilsvarende vis vil foregå via selvbetjeningsløsningen virk.dk, og at hændelsesunderretningen efter indgivelsen automatisk vil blive fordelt til de myndigheder og/eller sektorer, der er angivet som modtager af indberetningen.

2.2.8. Straf

Dansk Industri opfordrer til, at der i lovbemærkningerne tages højde for, at der skal være det nødvendige råderum for domstolene til at udmåle bødestraffen på grundlag af den enkelte sags konkrete

omstændigheder, og derved ikke "fastlåses" til at gøre brug af forudsatte beløbsgrænser.

Ministeriet for Samfundssikkerhed og Beredskab har noteret sig bemærkninger.

Ministeriet bemærker, at der ved pålæg af en bøde og ved udmåling af bødens størrelse lægges vægt på 1) overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende ... under alle omstændigheder skal betragtes som alvorlige overtrædelser: a) gentagne overtrædelser, b) manglende underretning om eller afhjælpning af væsentlige hændelser, c) manglende afhjælpning af mangler efter bindende instrukser fra kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, 2) overtrædelsens varighed, 3) den pågældende enheds relevante tidligere overtrædelser, 4) enhver materiel eller immateriel skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den materielle eller immaterielle skade, 7) hvorvidt gopdkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med de kompetente myndigheder. Det fremgår endvidere, at en fastsat bøde skal være effektiv, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning under hensyntagen til omstændighederne i den konkrete sag.

Ministeriet for Samfundssikkerhed og Beredskab har nu præciseret i lovforslaget, at fastsættelsen af straffen vil bero på domstolenes konkrete vurdering i det enkelte tilfælde af samtlige omstændigheder i sagen, og de angivne strafniveauer vil kunne fraviges i op- eller nedadgående retning, hvis der i den konkrete sag foreligger skærpende eller formildende omstændigheder, jf. herved de almindelige regler om straffens fastsættelse i straffelovens 10. kapitel.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 32.

2.2.9. Økonomiske- og administrative byrder

ATP, Dansk Industri, Danske Regioner, DANVA, TEKNIQ Arbejdsgiverne opfordrer til, at der foretages en ny kvantificering af de erhvervsøkonomiske konsekvenser ved lovforslaget, når de sektorspecifikke bekendtgørelser foreligger.

Det fremgår af lovforslagets pkt. 6, at lovforslaget forventes at medføre væsentlige negative erhvervsøkonomiske konsekvenser for ca. 3.255 virksomheder i Danmark. Bl.a. vil virksomheder skulle overholde registrerings- og underretningsforpligtelserne i de foreslåede §§ 9, 10, 12 og 13 i lovforslaget.

Lovforslaget stiller derudover i § 6 krav om, at enheder skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operation eller til at levere deres tjenester.

NIS 2-hovedloven medfører en række administrative krav for private virksomheder. Med afsæt i data fra Klima-, Energi- og Forsyningsministeriets AMVAB-undersøgelse for bekendtgørelse om modstandsdygtighed og beredskab i energisektoren skønnes de administrative omkostninger ved nærværende lovforslag med stor usikkerhed at udgøre ca. 2,8-3,3 mia. kr. i omstillingsomkostninger og ca. 0,7-1,2 mia. kr. årligt i løbende udgifter.

Ligeledes medfører lovforslaget en række øvrige efterlevelseskonsekvenser for private virksomheder. Med afsæt i Klima-, Energi- og Forsyningsministeriets erhvervsøkonomiske konsekvenser for bekendtgørelse om modstandsdygtighed og beredskab i energisektoren skønnes de øvrige efterlevelsesomkostninger ved nærværende lovforslag med stor usikkerhed at udgøre 1,6-2,4 mia. kr. i omstillingsomkostninger og 2,0-2,6 mia. kr. i løbende udgifter

Som det fremgår af lovforslagets pkt. 6, vil der efter lovens ikrafttræden blive gennemført en AMVAB-måling af de administrative konsekvenser ligesom at de øvrige efterlevelseskonsekvenser genberegnes. Det bemærkes, at der udestår en kvantificering af de samlede erhvervsøkonomiske konsekvenser for leverandører til de virksomheder, der er omfattet af loven. Disse vil indgå i målingen efter lovens ikrafttræden.

3. Lovforslaget i forhold til lovudkastet

I forhold til det udkast til lovforslag, der har været i offentlig høring, indeholder det fremsatte lovforslag følgende indholdsmæssige ændringer:

- Der er indsat en definition af en nærvedhændelse i den foreslåede § 3, nr. 21.
- Der er indsat en definition af 'sikkerhed i net- og informationssystemer' i den foreslåede § 3, nr. 27.
- Der er foretaget en korrektion af størrelseskravet i de foreslåede bestemmelser i §§ 4, stk. 1 og 2 og 5, stk. 1.
- Der er indsat en ny bemyndigelsesbestemmelse i den foreslåede § 20, stk. 3, der bemyndiger ministeren for samfundssikkerhed og beredskab til at fastsætte regler om koordinering, ansvar, fordeling af opgaver og udveksling af oplysninger mellem henholdsvis de kompetente myndigheder samt de kompetente myndigheder og CSIRT'en, herunder i forhold til hændelsesunderretninger efter kapitel 3, tilsyn samt håndhævelse efter kapitel 6.
- Der er indsat to nye håndhævelsesforanstaltninger i §§ 22, stk. 1, nr. 1 og 2, og 25, stk. 1, nr. 1 og 2, der giver de kompetente myndigheder mulighed for at anvende advarsler og bindende instrukser som håndhævelsesforanstaltninger.
- Der er blevet indsat en ny bestemmelse i den foreslåede § 33, stk. 2, hvorefter ministeren for samfundssikkerhed og

beredskab senest 3 år efter lovens ikrafttræden udarbejder en rapport om erfaringerne med loven.

Herudover er der foretaget ændringer af sproglig, redaktionel og lovteknisk karakter.