FORSVARSMINISTERIET
MINISTRY OF DEFENCE

U d k a s t

Forslag
til
Lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.[1]

Kapitel 1
Definitioner og anvendelsesområde

§ 1. I denne lov forstås ved:

1) Internetudvekslingspunkt: En netfacilitet, der muliggør sammenkobling af mere end to uafhængige autonome systemer, hovedsagligt med henblik på at lette udvekslingen af internettrafik.
2) Net- og informationssystem:
   a) Elektroniske kommunikationsnet i form af radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af tjenester,
   b) enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller
   c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.
3) Sikkerhed i net- og informationssystemer: Evnen for net- og informationssystemer til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.
4) Hændelse: Enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.
5) Operatør af væsentligt internetudvekslingspunkt: En enhed, der leverer tjenester i form af internetudvekslingspunkter, hvor:
   a) Tjenesten er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,
   b) leveringen af denne tjeneste afhænger af net- og informationssystemer, og
   c) en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

[1] Loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2016/1148 (EU) af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EU-Tidende 2016, nr. L 194, side 1.

6) Digital tjeneste: Enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager, og som er af typen online-markedsplads, online-søgemaskine eller cloud computing-tjeneste.
7) Udbyder af digital tjeneste: Enhver juridisk person, som udbyder en digital tjeneste, og som har hovedsæde eller en repræsentant i Danmark.
8) Nationalt centralt kontaktpunkt: En national kompetent enhed med ansvar for at koordinere spørgsmål vedrørende sikkerheden i net- og informationssystemer samt grænseoverskridende samarbejde i EU herom.
9) CSIRT: En national it-beredskabsenhed, der håndterer hændelser, og som har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU.
10) CSIRT-netværket: Et netværk bestående af repræsentanter fra EU-medlemsstaternes CSIRT'er, og som har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU.

§ 2. Loven finder ikke anvendelse på operatører af væsentlige internetudvekslingspunkter, der er omfattet af lov om net- og informationssikkerhed.

Kapitel 2
Sikkerhed i net- og informationssystemer

§ 3. Center for Cybersikkerhed fastsætter regler om minimumskrav til sikkerheden i net- og informationssystemer for væsentlige operatører af internetudvekslingspunkter. Reglerne kan omfatte krav om passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som operatører af væsentlige internetudvekslingspunkter anvender til deres aktiviteter. Reglerne kan endvidere omfatte krav om passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer, som operatører af væsentlige internetudvekslingspunkter anvender til levering af væsentlige tjenester med henblik på at sikre kontinuiteten i disse tjenester. Der kan fastsættes krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Stk. 2. Center for Cybersikkerhed kan påbyde operatører af væsentlige internetudvekslingspunkter at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net- og informationssystemer i deres processer efter stk. 1.

Stk. 3. Center for Cybersikkerhed kan påbyde operatører af væsentlige internetudvekslingspunkter at afhjælpe nærmere påviste mangler i relation til sikkerheden i deres net- og informationssystemer.

§ 4. Center for Cybersikkerhed fastsætter regler om operatører af væsentlige internetudvekslingspunkters underretning af Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som operatørerne leverer. Center for Cybersikkerhed kan i den forbindelse fastsætte krav om, hvordan og i hvilken form oplysningerne skal afgives.

Kapitel 3
Tilsyn m.v.

§ 5. Center for Cybersikkerhed fører tilsyn med overholdelsen af denne lov og regler, der er udstedt i medfør af loven.

Stk. 2. Center for Cybersikkerhed kan som led i sit tilsyn kræve, at operatører af væsentlige internetudvekslingspunkter fremlægger alle de oplysninger og det materiale, der er nødvendige for centerets tilsynsvirksomhed, herunder til afgørelse af, om et forhold falder ind under denne lov eller regler, der er udstedt i medfør af denne lov.

Stk. 3. Center for Cybersikkerhed kan stille krav om, hvordan og i hvilken form oplysninger og materiale efter stk. 2 skal afgives.

§ 6. Center for Cybersikkerhed kan orientere offentligheden om en hændelse, som centeret har modtaget underretning om efter § 4, hvis offentlighedens kendskab til hændelsen er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse. Forud for orientering af offentligheden hører Center for Cybersikkerhed den operatør af et væsentligt internetudvekslingspunkt, der har underrettet om hændelsen.

Stk. 2. Center for Cybersikkerhed kan i koordination med de relevante tilsynsmyndigheder i andre sektorer og efter forudgående høring af de operatører af væsentlige tjenester, der har underrettet om hændelsen, orientere offentligheden om hændelser, der berører flere samfundsvigtige sektorer, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Stk. 3. Center for Cybersikkerhed kan i koordination med de relevante tilsynsmyndigheder i andre sektorer og efter forudgående høring af de udbydere af digitale tjenester, der har underrettet om hændelsen, orientere offentligheden om hændelser, der berører flere samfundsvigtige sektorer, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse af hændelsen i øvrigt er i offentlighedens interesse.

Stk. 4. Center for Cybersikkerheds orientering af offentligheden efter stk. 1-3 må ikke indeholde

1) oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el. lign. for så vidt det er af væsentlig betydning for den udbyder af digitale tjenester eller operatør af væsentlige tjenester, som oplysningerne angår,
2) oplysninger, der er af væsentlig betydning for statens sikkerhed eller rigets forsvar,
3) klassificerede informationer, eller
4) oplysninger om enkeltpersoners forhold.

§ 7. Center for Cybersikkerhed kan i forbindelse med modtagelse af underretninger om hændelser af grænseoverskridende karakter fra tilsynsmyndigheder i andre sektorer, operatører af tjenester og udbydere af digitale tjenester videregive oplysninger om disse hændelser til nationale tilsynsmyndigheder, CSIRT'er og nationale centrale kontaktpunkter i andre EU-medlemsstater samt CSIRT-netværket.

Stk. 2. Center for Cybersikkerhed orienterer de operatører af tjenester samt udbydere af digitale tjenester, som underretningerne hidrører fra, om videregivelse efter stk. 1.

§ 8. Center for Cybersikkerhed kan fastsætte regler om, at skriftlig kommunikation til og fra centeret om nærmere bestemte forhold, som er omfattet af denne lov eller af regler udstedt i medfør af denne lov, skal foregå digitalt.

Stk. 2. Center for Cybersikkerhed kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur el.lign.

Stk. 3. En digital meddelelse anses for at være kommet frem, når den er tilgængelig for adressaten for meddelelsen.

Kapitel 4
Straffebestemmelser

§ 9. Med bøde straffes, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der

1) undlader at efterkomme Center for Cybersikkerheds påbud efter § 3, stk. 2 og 3, eller
2) undlader at efterkomme Center for Cybersikkerheds krav efter § 5, stk. 2.

Stk. 2. I regler, som udfærdiges i medfør af § 3, stk. 1, og § 4, kan der fastsættes straf i form af bøde for overtrædelse af bestemmelserne i reglerne.

Stk. 3. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Kapitel 5
Ikrafttræden m.v.

§ 10. Loven træder i kraft den 9. maj 2018.

§ 11. Loven gælder ikke for Færøerne og Grønland.

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning og formål

Europa-parlamentet og Rådet har vedtaget direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet).

NIS-direktivet stiller fælles sikkerhedskrav til operatører af væsentlige tjenester og udbydere af digitale tjenester inden for en række samfundsvigtige sektorer, som bl.a. omfatter energi, transport, bankvæsen, finansielle markedsinfrastrukturer, sundhed, drikkevandsforsyning og -distribution samt digital infrastruktur. Samtidig fastsættes krav om underretning af myndighederne ved hændelser, som har negativ indvirkning på sikkerheden i net- og informationssystemer.

Baggrunden for NIS-direktivet er, at net- og informationssystemer i dag spiller en afgørende rolle i samfundet. Det er således i høj grad en forudsætning for de økonomiske og samfundsmæssige aktiviteter, at net- og informationssystemerne i de samfundsvigtige sektorer er pålidelige og sikre. Samtidig er både omfanget, hyppigheden og konsekvenserne af sikkerhedshændelser tiltagende, således at de udgør en alvorlig trussel for driften af net- og informationssystemer. Hertil kommer, at systemerne kan blive mål for egentlige angreb, der har til formål at ødelægge eller forstyrre systemernes drift.

NIS-direktivet skal være implementeret i dansk ret senest den 9. maj 2018. Direktivet vil blive implementeret individuelt i de enkelte sektorer, som er omfattet af direktivet, hvilket vil sikre, at der ved implementeringen fastsættes målrettede sikkerhedskrav, der er nøje tilpasset de enkelte sektorers særlige forhold. Dermed opnås den bedst mulige beskyttelse af net- og informationssystemer, mens erhvervslivet samtidig ikke pålægges unødigt bebyrdende krav.

Formålet med dette lovforslag er at implementere NIS-direktivet på Forsvarsministeriets område. Lovforslaget implementerer således de dele af direktivet, der vedrører sikkerhedskrav og underretningspligter på informationssikkerhedsområdet for de såkaldte internetudvekslingspunkter (Internet Exchange Points – IXP), som for så vidt angår informationssikkerhed henhører under Forsvarsministeriet. Herudover vil der med lovforslaget blive skabt de nødvendige forudsætninger for, at Center for Cybersikkerhed kan varetage en række tværgående myndighedsopgaver, som følger af direktivet, herunder varetage funktionen som centralt kontaktpunkt og beredskabsenhed, der håndterer it-sikkerhedshændelser (CSIRT).

2. Baggrund

2.1. Generelt om NIS-direktivet

NIS-direktivet har til formål at sikre et højt fælles sikkerhedsniveau for net- og informationssystemer inden for en række særligt samfundsvigtige sektorer i hele EU.

NIS-direktivet fastlægger for det første krav til rammerne for arbejdet med sikkerhed i net- og informationssystemer, både nationalt og på EU-niveau, herunder krav til samarbejdsorganer og myndig-

hedsstruktur. For det andet stiller NIS-direktivet krav om, at der fastsættes sikkerhedskrav og underretningspligter for operatører af væsentlige tjenester og udbydere af digitale tjenester.

2.1.1. Samarbejdsorganer og myndighedsstruktur

Med NIS-direktivet etableres der i EU-regi to samarbejdsfora, hvor medlemsstaterne er repræsenteret. Det ene forum er Samarbejdsgruppen, som fokuserer på det strategiske samarbejde mellem medlemsstaterne, mens det andet er CSIRT-netværket, som fokuserer på det operationelle samarbejde mellem medlemsstaternes CSIRT'er, der er de it-beredskabsenheder, som skal reagere på hændelser.

På nationalt plan forpligter NIS-direktivet medlemsstaterne til at udpege en eller flere nationale kompetente myndigheder, et nationalt centralt kontaktpunkt, samt en eller flere nationale CSIRT'er.

De nationale kompetente myndigheder fører tilsyn med anvendelsen af direktivet, og de betegnes derfor som tilsynsmyndigheder. I Danmark udpeger de relevante ressortmyndigheder de tilsynsmyndigheder, der skal føre tilsyn med de enkelte sektorer.

Det nationale centrale kontaktpunkt skal udgøre et forbindelsesled, som faciliterer det grænseoverskridende samarbejde med andre medlemsstater, Samarbejdsgruppen og CSIRT-netværket. Herudover skal det centrale kontaktpunkt én gang om året forelægge en sammenfattende rapport for Samarbejdsgruppen vedrørende underretninger om hændelser i henhold til NIS-direktivet. Center for Cybersikkerhed varetager funktionen som centralt kontaktpunkt i Danmark. Centeret, der er en del af Forsvarets Efterretningstjeneste, er i forvejen national it-sikkerhedsmyndighed og står for en forebyggende national rådgivnings- og oplysningsvirksomhed om cybersikkerhed i forhold til både den offentlige og private sektor samt en reaktiv indsats. Centeret varetager endvidere en række myndighedsopgaver og er således den centrale nationale myndighed vedrørende cybersikkerhed.

Udover at være nationalt centralt kontaktpunkt vil Center for Cybersikkerhed fremover varetage funktionen som Danmarks nationale CSIRT. Det indebærer, at centeret bl.a. skal løse følgende opgaver:

- Monitorering af hændelser på nationalt plan.
- Tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser.
- Reaktion på hændelser.
- Udarbejdelse af dynamiske risiko- og hændelsesanalyser og situationsrapporter.
- Deltagelse i CSIRT-netværket.
- Etablering af samarbejde med den private sektor.
- Fremme anvendelsen af fælles eller standardiserede procedurer for håndtering af hændelser og risici.
- Fremme anvendelsen af fælles eller standardiserede systemer til klassificering af hændelser, risici og oplysninger.

2.1.2. Krav til operatører af væsentlige tjenester og udbydere af digitale tjenester

NIS-direktivet stiller en række krav til gennemførelse af tekniske og organisatoriske sikkerhedsforanstaltninger samt underretning om væsentlige hændelser. Kravene er rettet mod operatører af væsentlige tjenester inden for energi, transport, bankvæsen, finansielle markedsinfrastrukturer, sundhedssektoren, drikkevandsforsyning og -distribution samt digital infrastruktur, samt mod udbydere af

digitale tjenester, som omfatter online-markedspladser, online-søgemaskiner og cloud computing-tjenester.

Det er de enkelte medlemsstater, som skal identificere de operatører, der leverer væsentlige tjenester og som dermed er omfattet af NIS-direktivets krav vedrørende sikkerhed i net- og informationssystemer. Der er i direktivet fastsat en række kriterier for identifikationen af disse operatører af væsentlige tjenester.

Operatører af væsentlige tjenester skal i medfør af NIS-direktivet hurtigst muligt underrette tilsynsmyndigheden eller den nationale CSIRT om hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som de leverer. På samme måde skal udbydere af digitale tjenester hurtigst muligt foretage en underretning til tilsynsmyndigheden eller den nationale CSIRT om enhver hændelse, der har betydelige konsekvenser for leveringen af en digital tjeneste, som de udbyder i Unionen.

Underretningerne skal bl.a. danne grundlag for, at tilsynsmyndighederne kan føre kontrol med operatører af væsentlige tjenester og udbydere af digitale tjenester inden for deres sektorer og evt. stille yderligere sikkerhedskrav til de pågældende operatører eller udbydere. Underretningerne skal endvidere give CSIRT'en grundlag for at reagere på hændelser samt danne grundlag for, at det centrale kontaktpunkt årligt kan forelægge Samarbejdsgruppen en sammenfattende rapport om modtagne underretninger. Herudover er underretningerne en forudsætning for, at tilsynsmyndigheden eller CSIRT'en kan orientere øvrige berørte medlemsstater om hændelser, der har grænseoverskridende konsekvenser.

De enkelte ressortmyndigheder fastsætter nærmere regler om sikkerhedskrav og underretningspligter inden for deres respektive sektorer og fører tilsyn med overholdelsen heraf. Det sikres i den forbindelse, at både tilsynsmyndigheden og CSIRT'en modtager underretningerne hurtigst muligt.

2.2. Sektorspecifik implementering

NIS-direktivet har et meget bredt anvendelsesområde, men forudsætningen for en målrettet og erhvervsvenlig direktivimplementering, hvor danske erhvervsvirksomheder ikke pålægges unødvendige byrder, er, at nye lovgivningskrav nøje tilpasses de enkelte sektorer. Ved implementeringen af NIS-direktivet videreføres sektoransvaret derfor, således at de enkelte ressortmyndigheder inden for eget område fortsat har ansvaret for at fastsætte og håndhæve de nødvendige regler om informationssikkerhed.

Implementeringen af NIS-direktivet vil således ske inden for en række forskellige ministerområder, hvoraf flere allerede har fastsat national regulering på informationssikkerhedsområdet. Da der endvidere er stor forskel på de sektorer, der er omfattet af direktivet, er det ikke muligt at fastlægge et fælles niveau for informationssikkerhed for alle de omfattede sektorer.

De enkelte ressortansvarlige myndigheder forestår implementeringen af direktivet inden for deres eget ressort, typisk ved at fremsætte lovforslag for Folketinget. I den forbindelse sikrer de ansvarlige myndigheder, at eventuel eksisterende lovgivning tilpasses, hvor det er nødvendigt, således at overlappende forpligtelser undgås, og erhvervsvirksomhederne ikke pålægges unødvendige byrder.

De ressortansvarlige myndigheder identificerer de operatører, der er væsentlige inden for den pågældende sektor, samt hvilke konkrete sikkerhedsforanstaltninger mv., der er relevante inden for sektoren.

På Forsvarsministeriets område implementerer lovforslaget dermed de dele af NIS-direktivet, der vedrører sikkerhedskrav og underretningspligter på informationssikkerhedsområdet for internetudvekslingspunkter samt de dele, der vedrører orientering af offentligheden om hændelser, der har en negativ indvirkning på sikkerheden i net- og informationssystemer, herunder orientering om tværgående hændelser, der ikke nødvendigvis har tilknytning til internetudvekslingspunkter.

3. Lovforslagets hovedindhold

3.1. Sikkerhedskrav og underretningspligter for operatører af væsentlige internetudvekslingspunkter

3.1.1. Gældende ret

På teleområdet er net- og informationssikkerhed reguleret ved lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed med tilhørende bekendtgørelser. Specifikt i relation til informationssikkerhed er der i medfør af loven udstedt bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester samt bekendtgørelse nr. 566 af 1. juni 2016 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

En del operatører af væsentlige internetudvekslingspunkter vil også kunne være teleudbydere, og i så fald vil de ikke være omfattet af lovforslaget, men i stedet (fortsat) være omfattet af lov om net- og informationssikkerheds sikkerhedskrav og underretningspligter. Øvrige operatører af væsentlige internetudvekslingspunkter er ikke på nuværende tidspunkt omfattet af regulering i forhold til sikkerheden i net- og informationssystemer.

3.1.2. Forsvarsministeriets overvejelser

Med lovforslaget implementeres NIS-direktivet, som har til formål at sikre et højt fælles sikkerhedsniveau for net- og informationssystemer, således at den stadigt stigende trussel mod net- og informationssystemer imødegås.

Sikkerhedskravene i NIS-direktivet omfatter overordnet en forpligtelse til at indføre risikostyringsprocesser, der kan sikre et højt sikkerhedsniveau i de pågældende tjenester. De omfattede operatører og udbydere skal træffe passende sikkerhedsforanstaltninger på baggrund af en vurdering af de risici, som virksomheden konkret står over for. Endvidere følger det af NIS-direktivet, at de omfattede operatører og udbydere hurtigst muligt skal underrette myndighederne om eventuelle hændelser, der har væsentlig forstyrrende virkning på levering af de pågældende tjenester.

Forsvarsministeriet lægger vægt på, at implementering af NIS-direktivet sker i overensstemmelse med regeringens principper for implementering af erhvervsrettet regulering, hvorefter den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen. Sikkerhedskrav og underretningspligter bør således nøje følge direktivets krav.

3.1.3. Den foreslåede ordning

Det foreslås i overensstemmelse med NIS-direktivet, at Center for Cybersikkerhed som myndighed på området kan fastsætte konkrete krav til operatører af væsentlige internetudvekslingspunkters sikkerhed i net- og informationssystemer.

Først og fremmest foreslås det, at Center for Cybersikkerhed bemyndiges til at fastsætte regler, som stiller krav om passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som operatører af væsentlige internetudvekslingspunkter anvender til deres aktiviteter. Herudover foreslås det, at reglerne kan omfatte krav om passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer, som operatører af væsentlige internetudvekslingspunkter anvender til levering af væsentlige tjenester med henblik på at sikre kontinuiteten i disse tjenester. Endvidere foreslås det, at der kan fastsættes krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer. Dette svarer i stort omfang til den regulering, der i dag gælder for teleudbydere i medfør af lov om net- og informationssikkerhed, om end der i forhold til teleudbydere stilles flere og mere detaljerede krav.

Det foreslås herudover, at Center for Cybersikkerhed kan påbyde operatører af væsentlige internetudvekslingspunkter at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net- og informationssystemer i deres processer. Det foreslås desuden, at Center for Cybersikkerhed kan påbyde operatører af væsentlige internetudvekslingspunkter at afhjælpe nærmere påviste mangler i relation til sikkerheden i deres net- og informationssystemer.

For så vidt angår underretningspligt foreslås det i overensstemmelse med NIS-direktivet, at Center for Cybersikkerhed kan fastsætte regler om operatører af væsentlige internetudvekslingspunkters underretning af Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som operatørerne leverer.

Der henvises til øvrigt til bemærkningerne til de foreslåede §§ 3 og 4.

3.2. Videregivelse og offentliggørelse af underretninger om væsentlige hændelser

3.2.1. Gældende ret

Der er ikke i gældende ret en specifik regulering af videregivelse og offentliggørelse af underretninger om hændelser fra operatører af væsentlige tjenester og udbydere af digitale tjenester på tværs af sektorer.

Danske forvaltningsmyndigheders videregivelse af oplysninger til en anden forvaltningsmyndighed vil dog være omfattet af persondataloven, såfremt der er tale om oplysninger om enkeltpersoner (personoplysninger), og forvaltningslovens § 28.

3.2.2. Forsvarsministeriets overvejelser

Det følger af NIS-direktivet, at operatører af væsentlige tjenester skal underrette tilsynsmyndigheden eller CSIRT'en om hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som de leverer. Det følger endvidere af direktivet, at udbydere af digitale tjenester skal underrette tilsynsmyndigheden eller CSIRT'en om hændelser, der har betydelige konsekvenser for leveringen af en tjeneste, som de udbyder i Unionen. Derudover kan enheder, der ikke er identificeret som operatører af væsentlige tjenester eller udbydere af digitale tjenester, på frivillig basis underrette om

hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som de leverer. Såfremt en hændelse har grænseoverskridende karakter, skal tilsynsmyndigheden eller CSIRT'en underrette andre berørte medlemsstater herom.

Uanset hvilken model for håndtering af underretninger, som vælges, er det både for tilsynsmyndighederne, CSIRT'en og det nationale centrale kontaktpunkt afgørende, at de hver især modtager underretninger fra operatører af væsentlige tjenester om hændelser, der har væsentlige konsekvenser for kontinuiteten af de leverede tjenester, og fra udbydere af digitale tjenester om hændelser, der har betydelige konsekvenser for leveringen af tjenesten.

Det vil være op til ressortmyndighederne indenfor de enkelte sektorer at fastsætte nærmere regler om underretning inden for deres respektive sektorer og føre tilsyn med overholdelsen heraf. Ressortmyndighederne sikrer i den forbindelse, at Center for Cybersikkerhed i sin funktion af CSIRT og nationalt centralt kontaktpunkt modtager de nødvendige underretninger.

Det vurderes som mest hensigtsmæssigt, at opgaven med at underrette andre EU-medlemsstater om hændelser af grænseoverskridende karakter placeres hos Center for Cybersikkerhed som led i centerets funktion som national CSIRT.

Forsvarsministeriet finder på den baggrund, at Center for Cybersikkerhed bør have en udtrykkelig hjemmel til at videregive de modtagne underretninger om hændelser af grænseoverskridende karakter til nationale tilsynsmyndigheder, CSIRT'er og nationale centrale kontaktpunkter i andre EU-medlemslande samt til CSIRT-netværket. Forsvarsministeriet finder i den forbindelse, at der bør ske orientering af den underrettende operatør eller udbyder af digitale tjenester i forbindelse med videregivelsen.

I medfør af NIS-direktivet skal det sikres, at den kompetente myndighed eller CSIRT'en efter høring af den pågældende operatør kan offentliggøre konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse. Offentliggørelsen skal ske under hensyntagen til bl.a. operatørens sikkerhed, operatørens kommercielle interesser og fortrolig behandling af de af operatøren angivne oplysninger i forbindelse med dennes underretning. Det samme gør sig gældende for så vidt angår udbydere af digitale tjenester. Det følger dog af direktivet, at der her ligeledes kan ske offentliggørelse, hvis offentliggørelse af hændelsen i øvrigt er i offentlighedens interesse.

Orientering af offentligheden om en konkret hændelse varetages af de enkelte tilsynsmyndigheder. For så vidt angår operatører af væsentlige internetudvekslingspunkter bør der således – i overensstemmelse med NIS-direktivet – skabes hjemmel til, at Center for Cybersikkerhed kan orientere offentligheden om en hændelse, som centeret har fået underretning om fra en operatør af væsentlige internetudvekslingspunkter.

Forsvarsministeriet finder derudover, at orienteringen af offentligheden i tilfælde, hvor en hændelse berører flere sektorer, bør foretages af Center for Cybersikkerhed i koordination med de relevante tilsynsmyndigheder.

3.2.3. Den foreslåede ordning

Det foreslås, at Center for Cybersikkerhed i forbindelse med modtagelse af underretninger om hændelser af grænseoverskridende karakter fra tilsynsmyndigheder i andre sektorer, operatører af tjene-

ster og udbydere af digitale tjenester kan videregive oplysninger om disse hændelser til nationale tilsynsmyndigheder, CSIRT'er og nationale centrale kontaktpunkter i andre EU-medlemsstater samt CSIRT-netværket.

Det foreslås endvidere, at Center for Cybersikkerhed i forbindelse med en sådan videregivelse orienterer den operatør af tjenester eller udbyder af digitale tjenester, som underretningerne hidrører fra.

I relation til operatører af væsentlige internetudvekslingspunkter foreslås det, at Center for Cybersikkerhed kan orientere offentligheden om en hændelse, som centeret har modtaget underretning om, hvis offentlighedens kendskab til hændelsen er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse. Forud for orientering af offentligheden hører Center for Cybersikkerhed den operatør af det væsentlige internetudvekslingspunkt, der har underrettet om hændelsen. Endvidere foreslås det, at Center for Cybersikkerhed i koordination med de relevante tilsynsmyndigheder og efter forudgående høring af de operatører af væsentlige tjenester, der har underrettet om hændelsen, kan orientere offentligheden om hændelser, der berører flere samfundsvigtige sektorer, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

For så vidt angår underretninger fra udbydere af digitale tjenester foreslås det, at Center for Cybersikkerhed i koordination med de relevante tilsynsmyndigheder og efter forudgående høring af de udbydere af digitale tjenester, der har underrettet om hændelsen, kan orientere offentligheden om hændelser, der berører flere samfundsvigtige sektorer, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse af hændelsen i øvrigt er i offentlighedens interesse.

Der henvises i øvrigt til bemærkningerne til de foreslåede §§ 6 og 7.

3.3. Tilsyn m.v.

3.3.1. Gældende ret

§ 9 i lov om net- og informationssikkerhed regulerer Center for Cybersikkerheds tilsyn med teleudbyderes overholdelse af loven og de bekendtgørelser, der er udstedt i medfør af loven.

De operatører af væsentlige internetudvekslingspunkter, der ikke samtidig er teleudbydere i lov om net- og informationssikkerheds forstand, er derimod ikke på nuværende tidspunkt underlagt tilsyn i forhold til sikkerheden i net- og informationssystemer.

3.3.2. Forsvarsministeriets overvejelser

Et velfungerende tilsyn med sikkerheden i net- og informationssystemer for internetudvekslingspunkter er en vigtig forudsætning for et højt sikkerhedsniveau på området.

Det følger af NIS-direktivet, at tilsynsmyndighederne skal føre tilsyn med anvendelsen af direktivet på nationalt plan. Det følger endvidere af direktivet, at tilsynsmyndighederne skal have beføjelser og midler til at pålægge operatørerne at levere de oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker og dokumentation for den faktiske gennemførelse af sikkerhedspolitikker.

Forsvarsministeriet finder i overensstemmelse hermed, at der bør fastsættes regler om, at Center for Cybersikkerhed fører tilsyn med overholdelsen af loven, og at centeret i den forbindelse bør tillægges de beføjelser og midler, der er nødvendige for centerets tilsynsvirksomhed.

3.3.3. Den foreslåede ordning

Det foreslås, at Center for Cybersikkerhed fører tilsyn med overholdelsen af loven og de regler, der udstedes i medfør af loven.

Endvidere foreslås det, at Center for Cybersikkerhed som led i sit tilsyn kan kræve, at operatører af væsentlige internetudvekslingspunkter fremlægger alle de oplysninger og det materiale, der er nødvendigt for centerets tilsynsvirksomhed, herunder til afgørelse om, hvorvidt et forhold falder ind under denne lov eller regler udstedt i medfør af loven. I forlængelse heraf vil centeret kunne stille krav om, hvordan og i hvilken form oplysninger og materiale skal indgives.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 5.

4. Økonomiske og administrative konsekvenser for stat, kommuner og regioner

Lovforslaget vil medføre, at Center for Cybersikkerhed fremover skal varetage opgaverne som tilsynsmyndighed for internetudvekslingspunkter, nationalt centralt kontaktpunkt og national CSIRT. Dette vil have økonomiske konsekvenser, men udgifterne til de nye opgaver vil blive afholdt inden for Forsvarsministeriets eksisterende økonomiske ramme.

Lovforslaget vurderes på den baggrund ikke at have økonomiske eller administrative konsekvenser for det offentlige.

5. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

Lovforslaget vil få økonomiske og administrative konsekvenser for operatører af væsentlige internetudvekslingspunkter, der efter den foreslåede § 3 vil blive omfattet af regler om minimumskrav til sikkerheden i net- og informationssystemer.

Endvidere vil lovforslaget medføre administrative byrder for operatører af væsentlige internetudvekslingspunkter, der efter den foreslåede § 4 vil blive omfattet af regler om underretning af Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som operatørerne leverer, ligesom Center for Cybersikkerhed som led i centerets tilsyn efter den foreslåede § 5 vil kunne kræve, at operatørerne fremlægger alle de oplysninger og det materiale, der er nødvendige for centerets tilsynsvirksomhed.

De økonomiske og administrative konsekvenser vil afhænge af operatørernes eksisterende sikkerhedsniveau. Det vurderes dog, at kun et yderst begrænset antal virksomheder vil blive omfattet af den nye regulering.

6. Administrative konsekvenser for borgere

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

8. Forholdet til EU-retten

Lovforslaget – og den bekendtgørelse, der vil blive udstedt i medfør af loven – indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2016/1148 (EU) af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EU-Tidende 2016, nr. L 194, side 1.

9. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslaget har i perioden fra 27. oktober 2017 til 24. november 2017 været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatrådet, Amnesty International, Danish Internet eXchange point (DIX), Dansk Erhverv, Dansk Industri (DI), Danske Advokater, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DI ITEK, Domstolsstyrelsen, Institut for Menneskerettigheder, Internet eXchange point of the Oresund Region (IXOR), IT Branchen, IT-Politisk Forening, KL, Netnod IX Copenhagen, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rådet for Digital Sikkerhed, Stockholm Internet eXchange AB (STHIX), Teleindustrien (TI) og The Neutral Internet Exchange (NL-ix).

10. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Lovforslaget vil få økonomiske konsekvenser for operatører af væsentlige internetudvekslingspunkter, der efter den foreslåede § 3 vil blive omfattet af regler om minimumskrav til sikkerheden i net- og informationssystemer. De økonomiske konsekvenser vil afhænge af operatørernes eksisterende sikkerhedsniveau.
Administrative konsekvenser for erhvervslivet	Ingen	Lovforslaget vil få administrative konsekvenser for operatører

		af væsentlige internetudvekslingspunkter, der efter den foreslåede § 3 vil blive omfattet af regler om minimumskrav til sikkerheden i net- og informationssystemer. Endvidere vil lovforslaget medføre administrative byrder for operatører af væsentlige internetudvekslingspunkter, der efter den foreslåede § 4 vil blive omfattet af regler om underretning af Center for Cybersikkerhed, ligesom Center for Cybersikkerhed som led i centerets tilsyn efter den foreslåede § 5 vil kunne kræve, at operatørerne fremlægger alle de oplysninger og det materiale, der er nødvendige for centerets tilsynsvirksomhed. De administrative konsekvenser vil afhænge af operatørernes eksisterende sikkerhedsniveau.
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget – og den bekendtgørelse, der vil blive udstedt i medfør af loven – indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2016/1148 (EU) af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EU-Tidende 2016, nr. L 194, side 1.	
Overimplementering af EU-retlige minimumsforpligtelser (sæt X)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Den foreslåede § 1 definerer 10 centrale begreber i loven. Definitionerne bygger på de tilsvarende definitioner i NIS-direktivets artikel 4.

Med *nr. 1* defineres "internetudvekslingspunkt" som en netfacilitet, der muliggør sammenkobling af mere end to uafhængige autonome systemer, hovedsageligt med henblik på at lette udvekslingen af internettrafik. Et internetudvekslingspunkt leverer kun sammenkobling til autonome systemer. Endvidere forudsætter et internetudvekslingspunkt ikke, at internettrafik, som bevæger sig mellem et givent par af deltagende autonome systemer, bevæger sig gennem et eventuelt tredje autonomt system, og det hverken ændrer eller forstyrrer en sådan trafik. Definitionen af internetudvekslingspunkter svarer til definitionen i artikel 4, nr. 13, i NIS-direktivet.

Med *nr. 2* defineres "net- og informationssystem" som a) et elektroniske kommunikationsnet i form af radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af tjenester, b) enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller c) digitale data, som lages, behandles, fremfindes eller overføres af elementer i litra a eller b med henblik på deres drift, brug, beskyttelse og vedligeholdelse. Definitionen af net- og informationssystem svarer til definitionen i artikel 4, nr. 1, i NIS-direktivet.

Med *nr. 3* defineres "sikkerhed i net- og informationssystemer" som evnen for net- og informationssystemer til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer. Definitionen af sikkerhed i net- og informationssystem svarer til definitionen i artikel 4, nr. 2, i NIS-direktivet.

Med *nr. 4* defineres "hændelse" som enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer. Definitionen af en hændelse svarer til definitionen i artikel 4, nr. 7, i NIS-direktivet.

Med *nr. 5* defineres "operatør af væsentligt internetudvekslingspunkt" som en enhed, der leverer tjenester i form af internetudvekslingspunkter, hvor tjenesten er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, leveringen af tjenesten afhænger af net- og informationssystemer, og en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

Ved fastlæggelse af, om en hændelse vil få væsentlig forstyrrende virkning, skal der for det første tages hensyn til antallet af brugere, der er afhængige af de tjenester, som udbydes af operatøren, for det andet afhængighed af tjenesten i andre sektorer omfattet af NIS-direktivet, for det tredje konsekvenserne, som en hændelse kan have med hensyn til omfang og varighed på økonomiske og samfundsmæssige aktiviteter eller den offentlige sikkerhed, for det fjerde operatørens markedsandel, for det femte den geografiske udbredelse med hensyn til det område, som kan berøres af en hændelse, og for det sjette operatørens betydning med henblik på at opretholde et tilstrækkeligt tjenesteniveau under hensyn til tilgængelige alternative måder til levering af denne tjeneste.

De konkrete kriterier for fastlæggelse af, om der er tale om en operatør af et væsentligt internetudvekslingspunkt, vil kunne indgå i de regler, der fastsættes i medfør af den foreslåede § 3, stk. 1.

Definitionen af en operatør af et væsentligt internetudvekslingspunkt bygger på definitionen i NIS-direktivets artikel 4, nr. 4, jf. artikel 5, stk. 2, og artikel 6, stk. 1.

Med *nr. 6* defineres "digital tjeneste" som enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager, og som er af typen online-markedsplads, online-søgemaskine eller cloud computing-tjeneste. Definitionen af en digital tjeneste svarer til definitionen i NIS-direktivets artikel 4, nr. 5.

Med *nr. 7* defineres "udbyder af digital tjeneste" som enhver juridisk person, som udbyder en digital tjeneste, og som har hovedsæde eller en repræsentant i Danmark. Definitionen af en udbyder af digital tjeneste bygger på definitionen i NIS-direktivets artikel 4, nr. 6 og 10.

Med *nr. 8* defineres "nationalt centralt kontaktpunkt" som en national kompetent enhed med ansvar for at koordinere spørgsmål vedrørende sikkerheden i net- og informationssystemer samt grænseoverskridende samarbejde i EU herom. Definitionen af det nationale centrale kontaktpunkt bygger på beskrivelsen heraf i NIS-direktivets artikel 8.

Med *nr. 9* defineres "CSIRT" som en national it-beredskabsenhed, der håndterer hændelser og har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU. Definitionen af CSIRT bygger på beskrivelsen heraf i NIS-direktivets artikel 9 og bilag 1.

Med *nr. 10* defineres "CSIRT-netværket" som et netværk bestående af repræsentanter fra EU-medlemsstaternes CSIRT'er, og som har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU. Definitionen af CSIRT-netværket bygger på beskrivelsen heraf i NIS-direktivets artikel 12.

Til § 2

Bestemmelsen indebærer, at loven ikke finder anvendelse på operatører af væsentlige internetudvekslingspunkter, der er omfattet af lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed med tilhørende bekendtgørelser.

Lov om net- og informationssikkerhed med tilhørende bekendtgørelser fastsætter bl.a. sikkerhedskrav og underretningspligter for udbydere af net og tjenester. Lov om net- og informationssikkerhed implementerer bl.a. dele af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) som senest ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009. Det følger af NIS-direktivets artikel 1, stk. 3, at de sikkerhedskrav og den underretningspligt, der er fastsat i NIS-direktivet, ikke anvendes for virksomheder, der er omfattet af kravene i artikel 13 a og b i rammedirektivet.

Udbydere af net og tjenester i lov om net- og informationssikkerheds forstand vil derfor ikke være omfattet af dette lovforslags anvendelsesområde. En udbyder af net- og tjenester defineres i lov om net- og informationssikkerhed som den, der med et kommercielt formål stiller produkter, elektroniske kommunikationsnet eller -tjenester til rådighed for andre.

Hvis en udbyder af net og tjenester helt eller delvist ejer en operatør af et væsentligt internetudvekslingspunkt, men uden at operatøren er samme juridiske person som udbyderen, vil operatøren være omfattet af lovforslaget. Det kan f.eks. være tilfældet, hvis internetudvekslingspunktet drives i et datterselskab eller associeret selskab med udbyderen som ejer eller delejer, herunder hvis flere udbydere i fællesskab driver et internetudvekslingspunkt. Hvis internetudvekslingspunktet derimod dri-

ves af samme juridiske person som udbyderen, vil internetudvekslingspunktets aktiviteter – på samme vis som udbyderens øvrige aktiviteter – være omfattet af lov om net- og informationssikkerhed.

Til § 3

Det foreslås med *stk. 1,* at Center for Cybersikkerhed bemyndiges til at fastsætte regler for operatører af væsentlige internetudvekslingspunkter om minimumskrav til sikkerheden i net- og informationssystemer.

Bestemmelsen implementerer NIS-direktivets artikel 14, stk. 1 og 2.

Der kan med hjemmel i bestemmelsen fastsættes krav om, at operatører af væsentlige internetudvekslingspunkter skal håndtere sikkerheden i net- og informationssystemer gennem dokumenterede og ledelsesforankrede processer, herunder risikostyringsprocesser. Den foreslåede bemyndigelse forudsættes anvendt til administrativt at fastsætte nærmere krav til processerne. Der kan således administrativt stilles krav om, at processerne skal fastlægges og gennemføres med udgangspunkt i en relevant og anerkendt international standard eller tilsvarende.

Der kan endvidere med hjemmel i bestemmelsen fastsættes krav om, at operatører af væsentlige internetudvekslingspunkter skal forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer med henblik på at sikre kontinuiteten i operatørens tjenester.

Efter *stk. 2* kan Center for Cybersikkerhed påbyde operatører af væsentlige internetudvekslingspunkter at inddrage nærmere angivne områder af deres virksomhed eller nærmere angivne trusler mod sikkerheden i net- og informationssystemer i deres risikostyringsprocesser. Bestemmelsen skal ses i sammenhæng med bestemmelsen i stk. 1, hvorefter der kan fastsættes krav om, at operatører af væsentlige internetudvekslingspunkter skal benytte risikostyringsprocesser til at håndtere sikkerheden i net- og informationssystemer.

Der kan efter den foreslåede bestemmelse stilles krav om, at operatørerne af væsentlige internetudvekslingspunkter i risikostyringsprocesserne skal tage højde for bestemte (konkrete eller generelle) trusler mod sikkerheden i net- og informationssystemer efter påbud fra Center for Cybersikkerhed. Det kan f.eks. ske på baggrund af de trusselsvurderinger, som løbende udarbejdes af Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste.

Endvidere kan Center for Cybersikkerhed ved påbud bestemme, at visse områder af en operatør af væsentlige internetudvekslingspunkters virksomhed, der er nærmere specificeret i påbuddet, skal være omfattet af risikostyringsprocesserne, hvis dette ikke i forvejen er tilfældet.

Efter *stk. 3* kan Center for Cybersikkerhed påbyde operatører af væsentlige internetudvekslingspunkter at afhjælpe nærmere påviste mangler i relation til sikkerheden i deres net- og informationssystemer.

Bestemmelsen implementerer NIS-direktivets artikel 15, stk. 3.

Center for Cybersikkerhed vil som led i sit tilsyn kunne konstatere konkrete mangler på baggrund af oplysninger, som er modtaget fra operatøren i medfør af den foreslåede § 5, stk. 2. Sådanne oplysninger vil eksempelvis kunne omfatte resultaterne af en sikkerhedsaudit gennemført af en kvalificeret auditør. I de tilfælde, hvor Center for Cybersikkerhed på baggrund af de modtagne oplysninger konstaterer en konkret mangel, vil Center for Cybersikkerhed kunne påbyde operatøren at afhjælpe manglen.

Der henvises i øvrigt til afsnit 3.1 i de almindelige bemærkninger.

Til § 4

Den foreslåede § 4 bemyndiger Center for Cybersikkerhed til at fastsætte regler om underretningspligt for operatører af væsentlige internetudvekslingspunkter.

Bestemmelsen implementerer NIS-direktivets artikel 14, stk. 3.

Der kan med hjemmel i den foreslåede bestemmelse fastsættes regler om, at operatører af væsentlige internetudvekslingspunkter hurtigst muligt skal underrette Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som operatørerne leverer. Underretningen skal indeholde oplysninger, der gør det muligt at fastslå hændelsens eventuelle grænseoverskridende karakter.

Ved fastlæggelsen af, hvornår en hændelse har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, vil der bl.a. – direkte eller indirekte – kunne lægges vægt på antallet af brugere, der berøres af den væsentlige tjeneste, hændelsens varighed samt den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.

I reglerne vil det endvidere kunne fastsættes, at såfremt en operatør er afhængig af en tredjepartsudbyder af digitale tjenester vedrørende leveringen af en tjeneste i form af internetudvekslingspunkter, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, underretter operatøren om alle væsentlige konsekvenser for de væsentlige internetudvekslingspunkters kontinuitet som følge af en hændelse, der berører den pågældende udbyder.

Ved hurtigst muligt forstås inden udgangen af den førstkommende arbejdsdag efter, at den væsentlige hændelse er erkendt af den pågældende operatør. Såfremt operatøren på dette tidspunkt ikke er i besiddelse af komplette oplysninger om hændelsen, vil operatøren kunne afgive en underretning, der indeholder de oplysninger, som er til rådighed.

Center for Cybersikkerhed kan endvidere med hjemmel i den foreslåede bestemmelse fastsætte krav om, hvordan og i hvilken form oplysningerne skal afgives til centeret. Der kan eksempelvis stilles krav om, at oplysninger og materiale skal afgives ved anvendelse af et nærmere bestemt skema eller skal afgives elektronisk i form af indsendelse af elektroniske dokumenter eller via indtastninger på en hjemmeside.

Der henvises i øvrigt til afsnit 3.1 i de almindelige bemærkninger.

Til § 5

Med bestemmelsen i *stk. 1* foreslås det, at Center for Cybersikkerhed fører tilsyn med overholdelsen af denne lov og regler, der er udstedt i medfør af loven.

Center for Cybersikkerhed sikres med det foreslåede *stk. 2* adgang til de oplysninger, der er nødvendige til gennemførelse af centerets tilsynsvirksomhed. Bestemmelsen implementerer NIS-direktivets artikel 15, stk. 2.

Efter stk. 2 kan Center for Cybersikkerhed hos operatøren kræve enhver oplysning og alt materiale af betydning for centerets tilsynsmyndighed. Sådant materiale kan eksempelvis omfatte dokumenterede sikkerhedspolitikker samt dokumentation for den faktiske gennemførelse af sikkerhedspolitikkerne. Materialet kan endvidere omfatte resultaterne af en sikkerhedsaudit udført af en kvalificeret auditør og den tilgrundliggende dokumentation.

Med bestemmelsen i *stk. 3* foreslås det, at Center for Cybersikkerhed kan stille krav om, hvordan og i hvilken form oplysninger og materiale skal afgives til centeret. Der kan eksempelvis stilles krav om, at oplysninger og materiale skal afgives elektronisk i form af indsendelse af elektroniske dokumenter eller via indtastninger på en hjemmeside.

Der henvises i øvrigt til afsnit 3.1 i de almindelige bemærkninger.

Til § 6

Med bestemmelsen i *stk. 1* kan Center for Cybersikkerhed orientere offentligheden om en hændelse, som centeret har modtaget underretning om fra en operatør af væsentlige internetudvekslingspunkter i medfør af det foreslåede § 4. En sådan offentliggørelse må kun finde sted, hvis offentlighedens kendskab til hændelsen er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse. Center for Cybersikkerhed vil endvidere forud for orienteringen af offentligheden skulle høre den operatør af væsentlige internetudvekslingspunkter, der har underrettet om hændelsen.

Bestemmelsen implementerer NIS-direktivets artikel 14, stk. 6.

Center for Cybersikkerhed vil som enhed, der håndterer it-sikkerhedshændelser (CSIRT) modtage underretninger fra operatører af væsentlige tjenester inden for alle de sektorer, som NIS-direktivet omfatter, herunder energi, transport, bankvæsen, finansielle markedsinfrastrukturer, sundhed, drikkevandsforsyning og -distribution samt digital infrastruktur. Efter *stk. 2* kan Center for Cybersikkerhed, såfremt en hændelse berører flere samfundsvigtige sektorer, orientere offentligheden om hændelsesunderretninger, som centeret modtager vedrørende operatører af væsentlige tjenester.

Center for Cybersikkerheds orientering af offentligheden skal ske i koordination med den eller de relevante tilsynsmyndigheder. Derudover skal offentlighedens kendskab til hændelsen være nødvendig for at forebygge en hændelse eller håndtere en igangværende hændelse. Center for Cybersikkerhed vil endvidere forud for orienteringen af offentligheden skulle høre den operatør af væsentlige tjenester, der har underrettet om hændelsen.

Efter *stk. 3* kan Center for Cybersikkerhed på tilsvarende vis i koordination med de relevante tilsynsmyndigheder og i relevant omfang orientere offentligheden om hændelser, der berører flere samfundsvigtige sektorer, og som udbydere af digitale tjenester har underrettet om. I disse tilfælde vil Center for Cybersikkerhed, udover de tilfælde, der er oplistet under stk. 2, også kunne orientere offentligheden om en hændelse, hvis det i øvrigt er i offentlighedens interesse.

Det foreslås med *stk. 4, nr. 1,* at offentliggørelsen efter stk. 1-3 ikke må indeholde oplysninger vedrørende tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig betydning for den udbyder af digitale tjenester eller operatør af væsentlige tjenester, som oplysningerne angår. Definitionen af oplysninger vedrørende tekniske indretninger m.v. skal forstås i overensstemmelse med § 30, nr. 2, i offentlighedsloven og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Efter *stk. 4, nr. 2*, vil oplysninger skulle undtages fra offentliggørelse i det omfang, det er af væsentlig betydning for statens sikkerhed eller rigets forsvar. Vurderingen af, hvornår offentliggørelse kan være af væsentlig betydning for statens sikkerhed eller rigets forsvar, skal foretages i overensstemmelse med principperne i § 31 i offentlighedsloven.

Desuden vil klassificerede informationer efter *stk. 4, nr. 3,* blive slettet i det materiale, der offentliggøres.

Endelig vil enkeltpersoners forhold efter *stk. 4, nr. 4,* blive slettet inden offentliggørelse. Det kan eksempelvis være oplysninger om navne, adresser eller telefonnumre, som vil skulle undtages fra offentliggørelsen.

Der henvises i øvrigt til afsnit 3.2 i de almindelige bemærkninger.

Til § 7

Det foreslås med *stk. 1*, at Center for Cybersikkerhed i forbindelse med modtagelse af underretninger om hændelser af grænseoverskridende karakter fra tilsynsmyndigheder i andre sektorer, operatører af tjenester og udbydere af digitale tjenester kan videregive oplysningerne til nationale tilsynsmyndigheder, CSIRT'er og centrale kontaktpunkter i andre EU-medlemsstater samt CSIRT-netværket. Videregivelsen vil ske under hensyntagen til den underrettende operatørs eller udbyders sikkerhed og kommercielle interesser. Videregivelsen vil også kunne omfatte de frivillige underretninger, som modtages af enheder, der ikke er identificeret som operatører af væsentlige tjenester eller udbydere af digitale tjenester.

Den foreslåede bestemmelse implementerer NIS-direktivets artikel 14, stk. 5, artikel 16, stk. 6, og artikel 20.

Efter det foreslåede s*tk. 2* skal operatører af tjenester, hvis oplysninger videregives efter stk. 1, orienteres om videregivelsen. Orienteringen skal tidsmæssigt ske i tilknytning til videregivelsen, men der stilles ikke krav om, at orienteringen skal ske forud for videregivelsen.

Der henvises i øvrigt til afsnit 3.2 i de almindelige bemærkninger.

Til § 8

Efter det foreslåede *stk. 1* kan Center for Cybersikkerhed fastsætte regler om, at skriftlig kommunikation til og fra Center for Cybersikkerhed skal foregå digitalt. Der kan med hjemmel i bestemmelsen fastsættes regler om, hvem der omfattes af pligten til at kommunikere digitalt med Center for Cybersikkerhed, om hvilke forhold, og på hvilken måde.

Det bemærkes i den forbindelse, at pligten til at kommunikere digitalt ikke vil omfatte klassificerede informationer. Baggrunden herfor er, at sikkerhedscirkulæret stiller en række krav til digital forsendelse af klassificerede informationer, herunder bl.a. krav om sikkerhedsgodkendelse af informationssystemer samt anvendelse af godkendt kryptoudstyr.

Bestemmelsen indebærer, at skriftlige henvendelser til Center for Cybersikkerhed om forhold, som er omfattet af et krav om digital kommunikation, ikke anses for behørigt modtaget af centeret, hvis de indsendes på anden vis end den foreskrevne digitale måde. Hvis en virksomhed retter henvendelse til Center for Cybersikkerhed på anden måde end den foreskrevne digitale måde, eksempelvis ved brev, følger det af den almindelige vejledningspligt, jf. forvaltningslovens § 7, stk. 2, at centeret skal vejlede om reglerne på området, herunder om pligten til at kommunikere digitalt.

Herudover indebærer bestemmelsen, at der kan fastsættes regler om, at en virksomhed, som retter henvendelse til Center for Cybersikkerhed, skal oplyse en e-mailadresse, som virksomheden kan kontaktes på i forbindelse med behandlingen af en konkret sag eller henvendelse til centeret. I den forbindelse kan der også pålægges den pågældende virksomhed en pligt til at underrette centeret om en eventuel ændring af e-mailadressen, inden den konkrete sag afsluttes eller henvendelsen besvares, medmindre e-mails automatisk bliver videresendt til den nye e-mailadresse.

Der kan desuden fastsættes regler om, at Center for Cybersikkerhed kan sende visse meddelelser samt afgørelser, herunder påbud, til virksomhedens digitale postkasse med de retsvirkninger, der følger af bekendtgørelse nr. 801 af 13. juni 2016 af lov om Digital Post fra offentlige afsendere.

Der kan endvidere fastsættes regler om fritagelse for pligten til digital kommunikation. Fritagelsesmuligheden tænkes navnlig anvendt, hvor det er påkrævet at anvende en dansk digital signatur, men hvor der er tale om en virksomhed med hjemsted i udlandet, og som dermed ikke kan få udstedt en dansk digital signatur. Det bemærkes i den forbindelse, at fritagelsesmuligheden er stærkt begrænset, idet der er tale om kommunikation om erhvervsforhold.

Det forhold, at en virksomheds computere ikke fungerer, at virksomheden har mistet koden til sin digitale signatur, eller at der opstår lignende hindringer, som det er op til virksomheden at overvinde, kan ikke føre til fritagelse for pligten til digital kommunikation. I så fald må den pågældende virksomhed eksempelvis anmode en rådgiver om at varetage kommunikationen på virksomhedens vegne.

Efter det foreslåede *stk. 2* kan der fastsættes regler om anvendelse af bestemte it-systemer, digitale formater og digital signatur eller lignende. Den foreslåede bestemmelse indebærer, at det kan gøres obligatorisk for virksomheder at anvende bestemte internetløsninger, herunder selvbetjeningsløsninger.

Det foreslåede *stk. 3* fastsætter, hvornår en digital meddelelse må anses for at være kommet frem til adressaten for meddelelsen. Forslaget indebærer, at meddelelser til eller fra Center for Cybersikkerhed, der sendes på den foreskrevne digitale måde, anses for at være kommet frem til adressaten på det tidspunkt, hvor meddelelsen er tilgængelig digitalt for adressaten. Dermed er der tale om samme retsvirkning som ved fysisk post, der anses for at være kommet frem, når den pågældende meddelelse m.v. er lagt i adressatens fysiske postkasse. En meddelelse vil normalt anses for at være kommet frem, når meddelelsen er tilgængelig digitalt for adressaten, således at vedkommende har mulighed for at behandle meddelelsen. Dette tidspunkt vil normalt blive registreret automatisk i adressatens it-system.

Til § 9

Den foreslåede bestemmelse implementerer artikel 21 i NIS-direktivet, hvorefter medlemsstaterne skal fastsætte bestemmelser om sanktioner for overtrædelse af bestemmelser fastsat i medfør af direktivet.

Efter den foreslåede bestemmelse i *stk. 1* kan undladelse af at efterkomme Center for Cybersikkerheds påbud efter § 3, stk. 2 eller 3, straffes med bøde. Endvidere kan undladelse af at efterkomme Center for Cybersikkerheds krav i forbindelse med centerets tilsynsvirksomhed efter § 5, stk. 2, straffes med bøde.

Center for Cybersikkerhed bemyndiges med den foreslåede bestemmelse i *stk. 2* til at fastsætte straf i form af bøde for overtrædelse af regler udstedt i medfør af § 3, stk. 1, og § 4.

Efter det foreslåede stk. 3 kan der pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel. Bestemmelsen indebærer, at der også i regler, som udfærdiges i medfør af loven, kan fastsættes regler om, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Til § 10

Bestemmelsen fastsætter tidspunktet for lovens ikrafttræden. Det foreslås, at loven træder i kraft den 9. maj 2018, som er implementeringsfristen for NIS-direktivet efter direktivets artikel 25.

Det bemærkes, at det følger af NIS-direktivets artikel 5, stk. 1, at medlemsstaterne senest den 9. november 2018 skal have identificeret de operatører af væsentlige tjenester, der er omfattet af NIS-direktivet og dermed implementeringen. Identifikationen vil således kunne ske i perioden fra 9. maj 2018 til 9. november 2018.

Til § 11

Bestemmelsen vedrører lovens territoriale gyldighed.

Den foreslåede bestemmelse indebærer, at loven ikke gælder for Færøerne og Grønland.