Forslag

til

Lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren[1]

Kapitel 1

Lovens område

§ 1. Loven gælder for operatører, der leverer væsentlige tjenester inden for sundhedssektoren med henblik på at sikre et højt sikkerhedsniveau i disses net- og informationssystemer.

Kapitel 2

Operatører af væsentlige tjenester

§ 2. En offentlig eller privat enhed, herunder en fysisk eller juridisk person, som er etableret i Danmark, betragtes som en operatør af en væsentlig tjeneste, hvis

1) enheden leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter inden for sundhedssektoren,
2) leveringen af denne tjeneste afhænger af net- og informationssystemer, og
3) en hændelse vil få væsentlig forstyrrende virkning for leveringen af den nævnte tjeneste.

Stk. 2. Operatører af væsentlige tjenester skal registrere sig hos Sundhedsdatastyrelsen, som fører fortegnelse over de pågældende operatører.

Stk. 3. Sundhedsdatastyrelsen udarbejder en liste over tjenester, der er væsentlige for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter.

Stk. 4. Sundhedsdatastyrelsen fastsætter nærmere regler om de i stk. 1 nævnte kriterier samt registreringsordningen efter stk. 2.

§ 3. Operatører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at sikre et højt sikkerhedsniveau for net- og informationssystemer, som anvendes til deres aktiviteter og med disse foranstaltninger opretholde et sikkerhedsniveau, der står i forhold til risikoen.

Stk. 2. Operatører af væsentlige tjenester skal træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer, som anvendes til levering af de væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester.

Stk. 3. Sundhedsdatastyrelsen fastsætter nærmere regler om de i stk. 1 og 2 anførte sikkerhedsforanstaltninger.

§ 4. Operatører af væsentlige tjenester skal hurtigst muligt underrette Sundhedsdatastyrelsen om hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som de leverer. Underretningen

[1] Loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EU-Tidende 2016, nr. L 194, side 1-30.

skal indeholde oplysninger, der gør det muligt for Sundhedsdatastyrelsen at klarlægge eventuelle grænseoverskridende konsekvenser af hændelsen.

Stk. 2. Med henblik på at fastlægge omfanget af en hændelses konsekvenser efter stk. 1 skal operatøren af en væsentlig tjeneste navnlig tage følgende kriterier i betragtning:

1) Antallet af brugere, der berøres af afbrydelsen af den væsentlige tjeneste
2) Hændelsens varighed
3) Den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.

Stk. 3. Hvis en operatør af en væsentlig tjeneste er afhængig af en udbyder af digitale tjenester, skal operatøren underrette Sundhedsdatastyrelsen om en hændelse, der berører udbyderen, såfremt hændelsen har væsentlige konsekvenser for kontinuiteten af operatørens levering af den væsentlige tjeneste.

Stk. 4. Sundhedsdatastyrelsen meddeler så vidt muligt relevante oplysninger til den underrettende operatør om opfølgningen på dennes underretning, herunder oplysninger der kan støtte en effektiv håndtering af hændelsen.

Stk. 5. Sundhedsdatastyrelsen kan efter høring af den underrettende operatør oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Stk. 6. Sundhedsdatastyrelsen fastsætter nærmere regler om underretning efter stk. 1 og 3 samt kriterierne for fastlæggelsen af omfanget af en hændelses konsekvenser efter stk. 2.

Kapitel 3

Tilsyn

§ 5. Sundhedsdatastyrelsen fører tilsyn med de forpligtelser, der påhviler operatører af væsentlige tjenester i henhold til denne lov.

[Det er under afklaring, hvem der skal føre tilsyn i tilfælde hvor en institution under Sundheds- og Ældreministeriet er en operatør af en væsentlige tjeneste.]

§ 6. Sundhedsdatastyrelsen kan som led i sit tilsyn kræve, at operatører af væsentlige tjenester stiller følgende oplysninger til rådighed:

1) De oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker.
2) Dokumentation for den faktiske gennemførelse af sikkerhedspolitikker.

Stk. 2. Sundhedsdatastyrelsens anmodning om oplysninger eller dokumentation efter stk. 1 skal angive formålet med anmodningen og anføre, hvilke oplysninger der kræves.

Stk. 3. Sundhedsdatastyrelsen kan påbyde operatører af væsentlige tjenester at afhjælpe påviste mangler i henhold til denne lov.

Stk. 4. Sundhedsministeren kan fastsætte nærmere regler om Sundhedsdatastyrelsens tilsyn med operatører af væsentlige tjenester.

§ 7. Sundhedsdatastyrelsens afgørelser efter § 6, stk. 3, kan påklages til Sundheds- og Ældreministeriet for så vidt angår retlige spørgsmål.

Kapitel 4

Sanktioner

§ 8. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde, den der
1) undlader at efterkomme kravene i § 3, stk. 1 og 2 eller som i forhold, der omfattes af loven, meddeler Sundhedsdatastyrelsen urigtige eller vildledende oplysninger, eller
2) undlader at efterkomme Sundhedsdatastyrelsen påbud efter § 6, stk. 3.

Stk. 2. [Stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder udestår]

Stk. 3. I regler, der udstedes i medfør af loven, kan der fastsættes straf i form af bøde.

Stk. 4. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Kapitel 5

Ikrafttræden m.v.

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

§ 10. Loven gælder ikke for Færøerne og Grønland, jf. dog stk. 2.

Stk. 2. Loven kan ved kongelig anordning sættes helt eller delvist i kraft for Færøerne og Grønland med de afvigelser, som de færøske og grønlandske forhold tilsiger.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Formålet med lovforslaget er at sikre et højt niveau for net- og informationssikkerhed inden for sundhedssektoren, herunder sygehuse, praksissektoren, kommunal pleje mv. Lovforslaget implementerer dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen inden for sundhedssektoren.

Med lovforslaget foreslås det, at operatører af væsentlige tjenester skal indføre sikkerhedskrav, herunder risikostyringsforanstaltninger, der kan sikre et højt sikkerhedsniveau i de pågældende tjenester. Lovforslaget er udarbejdet med henblik på at sikre, at operatører af væsentlige tjenester kun

underlægges proportionale krav, der ikke er unødvendigt byrdefulde. Lovforslaget overlader derfor operatører af væsentlige tjenester et vist skøn til selv at beslutte indholdet af deres risikostyringsforanstaltninger under hensyntagen til de risici, som operatørerne er udsat for, og det aktuelle trusselsbillede.

Endvidere foreslås der indført et krav om, at operatører af væsentlige tjenester skal underrette Sundhedsdatastyrelsen om hændelser, der har forstyrrende virkning på de pågældende tjenester.

Det følger af Den fællesoffentlige digitaliseringsstrategi 2016-2020, at statslige myndigheder, regioner og kommuner har forpligtet sig til at implementere principperne i ISO27001 som grundlag for arbejdet med informationssikkerhed. Inden for det offentlige er de eksisterende aftaler om sikkerhedsforanstaltninger således allerede i dag i overensstemmelse med NIS-direktivets formål, hvorfor loven medfører mindre forpligtelser for offentlige operatører af væsentlige tjenester.

1.1 Baggrund for lovforslaget

Den øgede digitalisering af det danske samfund indebærer, at net- og informationssikkerhed spiller en stadig mere afgørende rolle, også for sundhedssektoren. Det er i høj grad en forudsætning for de tjenester, der understøtter behandling og pleje i sundhedssektoren, at sikkerheden fungerer.

Omfanget, hyppigheden og konsekvenserne af sikkerhedshændelser er tiltagende. Det digitale område er således i højere grad blevet et mål for handlinger, som har til formål at ødelægge eller forstyrre driften af digitale systemer. Uanset om hændelserne er tilsigtede eller ej, kan forstyrrelser i sundhedssektoren have alvorlige konsekvenser. En hændelse kan fx være et cyberangreb eller en oversvømmelse af en operatørs serverrum, der hindrer operatørens tjenester i at fungere og hæmmer en hensigtsmæssig behandling, pleje og patientsikkerhed. Sikkerhedshændelser kan dermed underminere borgernes tillid til sundhedsvæsenet.

Lovforslaget implementerer dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (herefter NIS-direktivet) inden for sundhedssektoren. Det følger af NIS-direktivet, at tjenester, der leveres til sundhedssektoren, kan være af særlig samfundskritisk karakter. Ifølge NIS-direktivet skal loven træde i kraft den 10. maj 2018.

2. Lovforslagets hovedpunkter

2.1. Operatører af væsentlige tjenester

2.1.1. Gældende ret

Operatører af væsentlige tjenester i sundhedssektoren er ikke underlagt en retlig regulering i forhold til net- og informationssikkerhed.

2.1.2. NIS-direktivet

NIS-direktivets krav til operatører af væsentlige tjenester er et udtryk for en minimumharmonisering. Der er således et nationalt spillerum for at fastsætte yderligere krav til operatører af væsentlige tjenester.

2.1.2.1. Identificering af operatører af væsentlige tjenester

Det følger af NIS-direktivet, at medlemsstaterne senest den 9. november 2018 skal identificere operatører af væsentlige tjenester inden for de respektive sektorer. I forbindelse med identificeringen af operatører af væsentlige tjenester skal det indgå, om en enhed leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter, om leveringen af denne tjeneste afhænger af net- og informationssystemer, og om en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

Hver medlemsstat skal udarbejde en liste over væsentlige tjenester inden for de af direktivet omfattede sektorer med henblik på at identificere operatører af væsentlige tjenester. Listen over væsentlige tjenester skal revideres og ajourføres hvert andet år efter den 9. maj 2018.

2.1.2.2. Sikkerhedskrav

Medlemsstaterne skal i henhold til NIS-direktivet sikre, at operatører af væsentlige tjenester træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at sikre et højt sikkerhedsniveau i deres net- og informationssystemer, som de anvender til deres aktiviteter. Sikkerhedsforanstaltningerne skal tage højde for det aktuelle teknologiske stade med det formål at sikre et sikkerhedsniveau, der står i forhold til risikoen. Medlemsstaterne skal desuden sikre, at operatører af væsentlige tjenester træffer passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i deres net- og informationssystemer med henblik på at opretholde kontinuiteten i deres tjenester.

2.1.2.3. Underretning om hændelser

Ifølge NIS-direktivet skal medlemsstaterne sikre, at operatører af væsentlige tjenester hurtigst muligt foretager en underretning til den kompetente myndighed og/eller Computer Security Incident Response Team (herefter CSIRT) om hændelser, der har væsentlige konsekvenser for kontinuiteten af deres tjenester. Underretningen skal indeholde oplysninger, der gør det muligt for den kompetente myndighed og/eller CSIRT at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. Vurderes hændelsen at have grænseoverskridende konsekvenser, underretter CSIRT relevante myndigheder i andre berørte medlemsstater om hændelsen. Underretningen til de berørte medlemsstater skal ske under overholdelse af krav om fortrolighed og sikkerhed. Ved fastlæggelsen af omfanget af en hændelses konsekvenser skal en operatør af en væsentlig tjeneste hovedsageligt tage hensyn til antallet af brugere, der berøres af afbrydelsen af den væsentlige tjeneste, hændelsens varighed og den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen. Yderligere skal der tages hensyn til antallet af sundhedspersoner og borgere, der berøres af operatørens virke pr. år samt betydningen for patientsikkerheden.

2.1.2.4. Offentliggørelse af hændelser

I henhold til NIS-direktivet kan den kompetente myndighed og CSIRT efter høring af operatøren af den væsentlige tjeneste offentliggøre konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendig 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.

2.1.3. Den foreslåede ordning

Lovforslaget har til hensigt at gennemføre NIS-direktivets bestemmelser for operatører af væsentlige tjenester inden for sundhedssektoren i dansk lovgivning.

2.1.3.1. Identificering af operatører af væsentlige tjenester

Det foreslås, at Sundhedsdatastyrelsen bemyndiges til at fastsætte de nærmere kriterier for identificeringen af operatører af væsentlige tjenester. Sundhedsdatastyrelsen bemyndiges endvidere til at udarbejde samt revidere og ajourføre listen over væsentlige tjenester, hvilket skal ske hver andet år efter den 9. maj 2018. Operatører af væsentlige tjenester skal registrere sig hos Sundhedsdatastyrelsen, som fører en fortegnelse over de pågældende operatører. At en operatør af en væsentlig tjeneste ikke har registreret sig hos Sundhedsdatastyrelsen, fritager ikke den pågældende operatør fra de forpligtelser, der følger af lovforslaget.

2.1.3.2. Sikkerhedskrav

Det foreslås, at der indføres krav om sikkerhedsforanstaltninger for operatører af væsentlige tjenester. Kravene vil indeholde de overordnede forpligtelser for operatører af væsentlige tjenester, således at operatørerne kan træffe de fornødne risikostyringsforanstaltninger. Det foreslås, at Sundhedsdatastyrelsen bemyndiges til at fastsætte nærmere regler om krav til sikkerhedsforanstaltninger. De nærmere fastsatte regler skal være i overensstemmelse med NIS-direktivets formål.

2.1.3.3. Underretning om hændelser

Det foreslås endvidere, at operatører af væsentlige tjenester skal underrette Sundhedsdatastyrelsen i tilfælde af hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Det foreslås, at Sundhedsdatastyrelsen bemyndiges til fastsætte de nærmere regler for, hvordan operatører af væsentlige tjenester skal underrette om hændelser til Sundhedsdatastyrelsen. Der vil ved fastsættelsen af sådanne regler være fokus på, at operatører af væsentlige tjenester kun underlægges proportionale krav, og, at de, i det omfang det er muligt, overlades et skøn til selv at beslutte indholdet i deres sikkerhedsstrategier.

2.1.3.4. Offentliggørelse af hændelser

Det foreslås, at Sundhedsdatastyrelsen kan orientere offentligheden om konkrete hændelser, efter høring af den berørte operatør, hvis offentlighedens kendskab hertil er nødvendig for at forebygge eller håndtere en igangværende hændelse.

2.2. Tilsyn

2.2.1. Gældende ret

Operatører af væsentlige tjenester i sundhedssektoren er ikke underlagt tilsyn i forhold til net- og informationssikkerhed.

2.2.2. NIS-direktivet

Direktivet foreskriver, at medlemsstaterne skal sikre, at de kompetente myndigheder har de nødvendige beføjelser og midler til at vurdere, hvorvidt operatører af væsentlige tjenester opfylder deres forpligtelser i henhold til direktivet. De kompetente myndigheder skal have beføjelser og midler til at pålægge operatørerne at levere de oplysninger, der nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker og dokumentation for den faktiske gennemførelse af sikkerhedspolitikker. Den kompetente myndigheds anmodning om oplysninger eller dokumentation skal indeholde en beskrivelse af formålet med anmodningen samt en angivelse af de oplysninger, der kræves. Med henblik på at afhjælpe mangler, kan den kompetente myndighed udstede påbud til operatører af væsentlige tjenester efter myndighedens vurdering af de indhentede oplysninger.

2.2.3. Den foreslåede ordning

Det foreslås, at Sundhedsdatastyrelsen skal føre tilsyn med overholdelsen af loven.

Sundhedsdatastyrelsen vil med lovforslaget få beføjelser til at kræve oplysninger af operatører af væsentlige tjenester, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer. Med henblik på at afhjælpe mangler, vil Sundhedsdatastyrelsen kunne udstede påbud til operatører af væsentlige tjenester herom. I forlængelse heraf vil Sundhedsdatastyrelsen som led i sit tilsyn med operatører få mulighed for at kræve dokumentation for den faktiske gennemførelse af sikkerhedspolitikker hos operatører af væsentlige tjenester.

[Det er under afklaring, hvem der skal føre tilsyn i tilfælde, hvor en institution inden for Sundheds- og Ældreministeriet er en operatør af en væsentlig tjeneste.]

3. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget vurderes ikke at medføre nye opgaver eller merudgifter af betydning i regioner og kommuner. Lovforslaget vurderes at medføre, at Sundhedsdatastyrelsen skal varetage nye opgaver, herunder bl.a. udarbejdelse samt revidering og ajourføring af listen over væsentlige tjenester, føre tilsyn med samt modtage underretninger om hændelser fra operatører af væsentlige tjenester. [Området for de statslige opgaver bevillingsfinansieres. Det kan, afhængigt at opgavens konkrete omfang, blive relevant at indføre gebyrordning, bl.a. henset til udviklingen i omfanget af tilsynsopgaver.]

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

Lovforslaget vurderes ikke at medføre væsentlige økonomiske konsekvenser for erhvervslivet.

Der vil være administrative konsekvenser for erhvervslivet i form af krav målrettet de private operatører i markedet, herunder registrering af operatører til Sundhedsdatastyrelsen, indberetning af hændelser, samt administrative aktiviteter i forbindelse med tilsyn. De administrative konsekvenser vurderes nærmere af Erhvervsstyrelsen Team Effektiv Regulering i forbindelse med udmøntningen i

de efterfølgende bekendtgørelser, når de konkrete oplysningskrav og omfanget af berørte virksomheder er kendt.

5. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

6. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

7. Forholdet til EU-retten

Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

8. Hørte myndigheder og organisationer

Et udkast til lovforslag har i perioden den 18. oktober 2017 til den 15. november 2017 været sendt i høring hos følgende myndigheder og organisationer m.v.:
3F, Ansatte Tandlægers Organisation, Brancheforeningen for Private Hospitaler og Klinikker, Danmarks Apotekerforening, Danmarks Optikerforening, Dansk Erhverv, Dansk Industri, Dansk IT – Råd for IT-og persondatasikkerhed, Dansk Kiropraktor Forening, Dansk Psykolog Forening, Dansk Psykoterapeutforening, Dansk Socialrådgiverforening, Dansk Standard, Dansk Sygeplejeråd, Dansk Tandplejerforening, Danske Bandagister, Danske Bioanalytikere, Danske Dental Laboratorier, Danske Fodterapeuter, Danske Fysioterapeuter, Danske Patienter, Danske Regioner, Datatilsynet, De Offentlige Tandlæger, Den Danske Dyrlægeforening, Ergoterapeutforeningen, Farmakonomforeningen, FOA, Forbrugerrådet, Foreningen af Kliniske Diætister, Foreningen af Speciallæger, Forsikring & Pension, Færøernes Landsstyre, Grønlands Selvstyre, Jordemoderforeningen, KL, Konkurrence- og Forbrugerstyrelsen, Københavns Universitet, Landsforeningen af Kliniske Tandteknikere, Lægeforeningen, Lægemiddelstyrelsen, Organisationen af Lægevidenskabelige Selskaber, Patienterstatningen, Praktiserende Lægers Organisation, Praktiserende Tandlægers Organisation, Psykologanævnet, Radiograf Rådet, Region Hovedstaden, Region Midtjylland, Region Nordjylland, Region Sjælland, Region Syddanmark, Rigsadvokaten, Rigsombudsmanden på Færøerne, Rigsombudsmanden på Grønland, Rigspolitiet, Roskilde Universitet, Rådet for Digital Sikkerhed, Socialpædagogernes Landsforbund, Statens Serum Institut, Styrelsen for Patientsikkerhed, Sundhedsdatastyrelsen, Sundhedsstyrelsen, Sundhedsstyrelsen, Strålebeskyttelse, Syddanmarks Universitet, Tandlægeforeningen, Tandlægeforeningens Tandskadeerstatning, Yngre Læger, Ældresagen, Aalborg Universitet, Aarhus Universitet.

9. Sammenfattende skema

	Positive konsekvenser/mindre udgifter (hvis ja, angiv omfang)	**Negative konsekvenser/merudgifter (hvis ja, angiv omfang)**
Økonomiske konsekvenser for det offentlige	Afværge hændelser og reducere konsekvenser af hændelser	Området for de nye statslige opgaver bevillingsfinansieres. Det kan afhængigt at opgavens konkrete omfang blive relevant at indføre gebyrordning.
Administrative konsekvenser for stat, regioner og kommuner	Stærk procedure for opfølgning på og rapportering af hændelser.	Sundhedsdatastyrelsen skal udarbejde samt revidere og ajourføre listen over væsentlige tjenester, føre tilsyn med og modtage underretninger fra operatører af væsentlige tjenester samt være i dialog med CFCS herom. Stat, regioner og kommuner, der er operatører af væsentlige tjenester skal underrette Sundhedsdatastyrelsen om hændelser, der har væsentlige konsekvenser for kontinuiteten af deres tjenester samt lade sig registrere.
Økonomiske konsekvenser for erhvervslivet mv.	Afværge og reducere hændelser samt en skærpet opmærksomhed på net- og informationssikkerhed.	I det omfang at der er private operatører af væsentlige tjenester, skal disse træffe passende sikkerhedsforanstaltninger
Administrative konsekvenser for erhvervslivet mv.	Ingen	Lovforslaget medfører administrative byrder for erhvervslivet. En nærmere vurdering af disse foretages af Erhvervsstyrelsens Team Effektiv Regulering i forbindelse med udarbejdelsen af de bekendtgørelser, der måtte følge af lovforslaget.

Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, gennemfører dele af Europa- Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.	
Overimplementering af EU-retlige minimumsforpligtelser (sæt x)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til kapitel 1

Til § 1

Det foreslås, at lovforslaget gælder for operatører af væsentlige tjenester. Som anført i lovforslagets almindelige bemærkninger tilsigtes det med lovforslaget at sikre et højt sikkerhedsniveau for net- og informationssystemer. Det indebærer, at operatører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i deres net- og informationssystemer.

Ved *net- og informationssystemer* forstås enten a) et elektronisk kommunikationsnet som defineret i telelovens § 2, nr. 4, dvs. et elektronisk kommunikationsnet i form af en radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af elektroniske kommunikationstjenester, 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 ved brug af elementer i førnævnte punkt a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse. Definitionen af net- og informationssystemer bygger på NIS-direktivets artikel 4, nr. 1.

Ved *sikkerhed i net- og informationssystemer* forstås net- og informationssystemers evne 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 informationssystemer bygger på NIS-direktivet artikel 4, nr. 2.

Til § 2

Til stk. 1

Den foreslåede bestemmelse fastsætter, at der ved *operatør af en væsentlig tjeneste* skal forstås, den offentlige eller private enhed, herunder en fysisk eller juridisk person, der er etableret i Danmark, og som leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter, leveringen af denne tjeneste afhænger af net- og informationssystemer, og en hændelse vil få væsentlig forstyrrende virkning for leveringen af den nævnte tjeneste. I den gældende lovgivning findes der ikke nogen legal definition af dette begreb. Bestemmelsens definition bygger på NIS-direktivets artikel 4, nr. 4, og artikel 5, stk. 2, litra a-c. I afklaringen af, om en tjeneste er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter, kan en operatør tage udgangspunkt i den liste over væsentlige tjenester, som Sundhedsdatastyrelsen skal vedligeholde i henhold til lovforslagets § 2, stk. 4.

Ved *hændelse* forstås enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer. Definitionen af hændelse bygger på NIS-direktivets artikel 4, nr. 7. I vurderingen af, hvorvidt en hændelse har væsentlig forstyrrende virkning, skal en række faktorer

indgå, som f.eks. det antal brugere, der er afhængige af tjenesten til private eller erhvervsmæssige formål samt hændelsens betydning for patientsikkerheden. Til eksempel kan antallet af patienter under operatørens virke pr. år inddrages i vurderingen af, hvorvidt en hændelse har væsentlig forstyrrende virkning. I vurderingen af en hændelses omfang og varighed på økonomiske og samfundsmæssige aktiviteter eller den offentlige sikkerhed, vil ligeledes kunne indgå, hvor lang tid, der skønnes at ville gå, før afbrydelsen af tjenesten vil have negative konsekvenser.

Til stk. 2

Med den foreslåede bestemmelse i § 2, stk. 2, fastsættes det, at operatører af væsentlige tjenester skal lade sig registrere hos Sundhedsdatastyrelsen, som fører en fortegnelse over de pågældende operatører.

Det understreges, at det forhold at en operatør af en væsentlig tjeneste ikke har registreret sig hos Sundhedsdatastyrelsen, ikke fritager den pågældende operatør fra de forpligtelser, der følger af lovforslaget.

Til stk. 3

Den foreslåede bestemmelse fastsætter, at Sundhedsdatastyrelsen bemyndiges til at udarbejde en liste over tjenester, der er væsentlige for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter. Bestemmelsen bygger på NIS-direktivets artikel 5, stk. 3. Listen kan bidrage til identificering af operatører af væsentlige tjenester inden for sundhedssektoren. Leverer en operatør væsentlige og ikke-væsentlige tjenester, har operatøren på baggrund af listen mulighed for at holde de væsentlige tjenester adskilt fra de ikke-væsentlige tjenester. Den nærmere afgrænsning af væsentlige tjenester vil tage udgangspunkt i tjenester, der er vigtige for samfundets funktionalitet, og hvor en afbrydelse f.eks. vil hindre gennemførelsen af aktiviteter inden for sundhedssektoren, herunder bl.a. patientbehandling, samt underminere borgernes tillid, eller på anden måde gøre skade på samfundets interesser.

Til stk. 4

Med den foreslåede bestemmelse bemyndiges Sundhedsdatastyrelsen til at fastsætte nærmere regler for afgræsningen af kriterierne efter bestemmelsens stk. 1. Sundhedsdatastyrelsen bemyndiges endvidere til at fastsætte nærmere regler om registreringsordningen efter bestemmelsens stk. 2. Fastsættelsen af regler om afgrænsning af kriterierne for at være en operatør af en væsentlig tjeneste samt regler om registreringsordningen skal ske inden for rammerne af NIS-direktivet.

Til § 3

Til stk. 1

Den foreslåede bestemmelse fastsætter, at operatører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at sikre et højt sikkerhedsniveau i deres net- og informationssystemer. Det er ikke hensigten, at operatører af væsentlige tjenester skal pålægges uforholdsmæssigt store økonomiske og administrative byrder, hvorfor sikkerhedsforanstaltningerne skal stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende net- og informationssystem. Det forudsættes, at foranstaltningerne under hensyn til teknologiens aktuelle stade, vil tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som er forbundet med operatørens levering af den pågældende tjeneste. Bestemmelsen har sin baggrund i NIS-direktivets artikel 14, stk. 1. De af operatørerne trufne sikkerhedsforanstaltninger skal så vidt muligt basere sig på internationale sikkerhedsgodkendte standarder, f.eks. ISO27001.

Til stk. 2

Den foreslåede bestemmelse fastsætter, at operatører af væsentlige tjenester skal træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser i deres net- og informationssystemer, som de bruger til levering af deres tjenester. Det er ikke hensigten, at operatører af væsentlige tjenester skal pålægges uforholdsmæssigt store økonomiske og administrative byrder, hvorfor sikkerhedsforanstaltningerne skal stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende net- og informationssystem. Bestemmelsen bygger på NIS-direktivets artikel 14, stk. 2.

Lovforslagets § 3, stk. 1 og 2, skal ses i sammenhæng. Begge bestemmelser har til formål at fremme en risikostyringskultur, hvor der foretages risikovurderinger og gennemføres sikkerhedsforanstaltninger. De af operatørerne trufne sikkerhedsforanstaltninger skal så vidt muligt basere sig på internationale sikkerhedsgodkendte standarder, f.eks. 27001.

Til stk. 3

Med den foreslåede bestemmelse får Sundhedsdatastyrelsen bemyndigelse til at fastsætte nærmere regler om sikkerhedsforanstaltninger efter stk. 1 og stk. 2 inden for rammerne af NIS-direktivet. Det er hensigten at udstede en bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af net- og informationssystemer, der anvendes af operatører af væsentlige tjenester, med samme ikrafttræden som loven.

Den almindelige forpligtelse til at træffe passende foranstaltninger efter stk. 1 og stk. 2 gælder uanset udstedelsen af regler herom.

Til § 4

Til stk. 1

Den foreslåede bestemmelse fastslår, at operatører af væsentlige tjenester hurtigst muligt skal underrette Sundhedsdatastyrelsen om hændelser, der har væsentlige konsekvenser for kontinuiteten af leveringen af deres tjenester. For så vidt angår definitionen af en *hændelse*, henvises til bemærkningerne til § 2, stk. 1. At operatøren skal underrette Sundhedsdatastyrelsen hurtigst muligt betyder, at operatøren, under hensyntagen til arbejdet med at minimere konsekvenserne af hændelsen, skal foretage underretningen, så snart operatøren har de nødvendige oplysninger til at kunne vurdere omfanget af hændelsen. Operatører af væsentlige tjenester skal være særligt opmærksomme på at få underrettet hurtigt i tilfælde af hændelser, der kan grænseoverskridende konsekvenser eller hændelser, der berører flere sektorer. Underretningen vil ikke i sig selv føre til et øget ansvar for operatøren. Underretningen til Sundhedsdatastyrelsen skal bl.a. indeholde oplysninger, der gør Sundhedsdatastyrelsen i stand til at vurdere, om hændelsen har konsekvenser for andre medlemslande.

Til stk. 2

Den foreslåede bestemmelse fastsætter, at operatører af væsentlige tjenester skal inddrage hændelsens betydning for patientsikkerheden, antallet af brugere, der berøres af hændelsen, hændelsens varighed og hvor stort et geografisk område, der berøres af hændelsen i vurderingen af, hvor omfangsrig en hændelses konsekvenser er.

Til stk. 3

Den foreslåede bestemmelse fastsætter, at en operatør af en væsentlig tjeneste hurtigst skal foretage en underretning til Sundhedsdatastyrelsen, hvis operatørens net- og informationssystemer påvirkes af en hændelse, der berører en digital udbyders tjeneste, som operatøren er afhængig af.

En *digital udbyder* skal forstås som enhver juridisk person, som udbyder en digital tjeneste af følgende type: en onlinemarkedsplads, en onlinesøgemaskine eller en cloud computing-tjeneste. Definitionen af en digital udbyder bygger på NIS-direktivets artikel 4, nr. 6, samt NIS-direktivets bilag III. En operatør af en væsentlig tjeneste kan f.eks. være afhængig af en udbyder af en digital tjeneste på baggrund af et kontraktforhold.

Bestemmelsen har til formål at sikre, at Sundhedsdatastyrelsen får kendskab til hændelser og mangler i sikkerheden hos udbydere af digitale tjenester, der har en negativ indvirkning på operatører af væsentlige tjenester.

Til stk. 4

Den foreslåede bestemmelse fastsætter, at Sundhedsdatastyrelsen, så vidt muligt, hvis omstændighederne tillader det, kan meddele oplysninger om opfølgningen på operatørens underretning, herunder oplysninger der kan støtte en effektiv håndtering af hændelsen.

Bestemmelsen har til formål at sikre, at operatøren får en tilbagemelding, der kan understøtte operatørens videre arbejde med at begrænse hændelsen, hvis omstændighederne tillader det.

Til stk. 5

Med den foreslåede bestemmelse bemyndiges Sundhedsdatastyrelsen adgang til at offentliggøre hændelser, såfremt det vurderes, at offentliggørelse vil være nødvendigt for at kunne forebygge eller håndtere en hændelse. Offentliggørelse skal ske efter høring af operatøren, og Sundhedsdatastyrelsen skal foretage en afvejning af offentlighedens interesse i at blive informeret om de pågældende trusler over for operatørens interesse i ikke at lide kommerciel skade. Bestemmelsen bygger på NIS-direktivets artikel 14, stk. 5.

Til stk. 6

Med den foreslåede bestemmelse bemyndiges Sundhedsdatastyrelsen til at fastsætte de nærmere kriterier for, hvornår og hvordan en underretning skal ske, jf. bestemmelsens stk. 1 og 3. Bestemmelsen bemyndiger endvidere Sundhedsdatastyrelsen til at fastsætte kriterierne for fastlæggelsen af omfanget af en hændelses konsekvenser, jf. bestemmelsens stk. 2.

Til § 5

Den foreslåede bestemmelse fastslår, at Sundhedsdatastyrelsen skal føre tilsyn med, at operatører af væsentlige tjenester overholder de forpligtelser, der følger af lovforslaget, samt de regler, der udstedes i medfør heraf.

[Det er under afklaring, hvem der skal føre tilsyn i de tilfælde, hvor en institution inden for Sundheds- og Ældreministeriet er en operatør af en væsentlig tjeneste.]

Til § 6

Til stk. 1

Den foreslåede bestemmelse fastsætter rammerne for Sundhedsdatastyrelsens tilsyn med operatører af væsentlige tjenester. Med den foreslåede bestemmelse får Sundhedsdatastyrelsen mulighed for at anmode om de oplysninger, der er nødvendige for gennemførelsen af styrelsens tilsynsvirksomhed. Sådanne oplysninger kan være operatørens dokumenterede sikkerhedspolitik og dokumentation for den faktiske gennemførelse af sikkerhedspolitikker, f.eks. resultaterne af en sikkerhedsaudit udfør af Sundhedsdatastyrelsen eller en kvalificeret auditør.

Til stk. 2

Med den foreslåede bestemmelse pålægges Sundhedsdatastyrelsen at angive formålet med anmodningen om oplysningerne efter stk. 1, samt at angive, hvilke typer af oplysninger, der anmodes om.

Til stk. 3

Den foreslåede bestemmelse fastslår, at Sundhedsdatastyrelsen, på baggrund af de oplysninger som styrelsen modtager efter stk. 1, kan udstede påbud til en operatør om afhjælpning af påviste mangler, såfremt det konstateres, at en operatør ikke har efterlevet kravene til sikkerhedsforanstaltninger.

Til stk. 4

Den foreslåede bestemmelse fastsætter, at sundhedsministeren kan fastsætte nærmere regler for Sundhedsdatastyrelsens tilsyn med operatører af væsentlige tjenester.

Til § 7

Den foreslåede bestemmelse fastsætter, at afgørelser truffet af Sundhedsdatastyrelsen efter § 6, stk. 3, kan påklages til Sundheds- og Ældreministeriet for så vidt angår retlige spørgsmål. Retlige spørgsmål omfatter såvel skreven som uskreven ret, herunder offentligretlige grundsætninger. Prøvelsen omfatter, ud over en stillingtagen til sagens retlige spørgsmål og sagens faktum, også eventuelle faglige vurderinger i det omfang, dette er nødvendigt for at kunne tage stilling til lovligheden af Sundhedsdatastyrelsens afgørelse. Der er principielt ikke begrænsninger i Sundheds- og Ældreministeriets prøvelse af jus, men hvor den konkrete subsumption forudsætter en særlig fagkundskab, som ministeriet ikke er i besiddelse af, udviser ministeriet tilbageholdenhed i prøvelsen, medmindre en udtalelse fra sektormyndigheden kan tilvejebringe det fornødne præcise beslutningsgrundlag. Det falder uden for Sundheds- og Ældreministeriets beføjelser at tage stilling til Sundhedsdatastyrelsens skønsudøvelse i det omfang, skønnet er udøvet inden for de rammer, lovgivningen sætter. Sundheds- og Ældreministeriets prøvelse omfatter ikke spørgsmål om hensigtsmæssighed, herunder sagsbehandlingens tilrettelæggelse eller sagsbehandlingstiden i det omfang, sådanne spørgsmål ikke er reguleret i lovgivningen.

Til § 8

Til stk. 1

Den foreslåede bestemmelse fastslår, at medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde den, der undlader at efterkomme kravene i lovforslagets § 3, stk. 1 og 2, eller som i forhold, der omfattes af lovforslaget, meddeler Sundhedsdatastyrelsen urigtige eller vildledende oplysninger, eller undlader at efterkomme Sundhedsdatastyrelsen påbud efter lovforslagets § 6, stk. 3.

Til stk. 2

[Stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder udestår]

Til stk. 3

Den foreslåede bestemmelse fastslår, at der kan fastsættes bøde for regler, der udstedes i medfør af lovforslaget.

Til stk. 4

Den foreslåede bestemmelse fastslår, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens kapitel 5. 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 § 9

Den foreslåede bestemmelse fastsætter tidspunktet for lovens ikrafttræden. Bestemmelsen bygger på NIS-direktivets artikel 25, stk. 1, hvorefter medlemsstaterne skal vedtage og offentliggøre de love og administrative bestemmelser, der er nødvendige for at efterkomme direktivet, senest den 9. maj 2018. Det følger videre af artiklen, at disse love og bestemmelser skal anvendes fra den 10. maj 2018. Det foreslås derfor, at loven træder i kraft den 10. maj 2018.

Til § 10

Til stk. 1

Den foreslåede bestemmelse fastlægger, at loven ikke skal gælde for Færøerne og Grønland.

Til stk. 2

Den foreslåede bestemmelse fastslår, at loven ved kongelig anordning kan sættes helt eller delvis i kraft for Færøerne og Grønland med de afvigelser, som de færøske og grønlandske forhold tilsiger.