



Fremsat den 7. februar 2018 af sundhedsministeren (Ellen Trane Nørby)

## Forslag

til

# Lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren<sup>1)</sup>

### Kapitel 1

#### *Lovens anvendelsesområde og definitioner*

§ 1. Loven gælder for operatører af væsentlige tjenester inden for sundhedssektoren.

§ 2. I denne lov forstås ved:

- 1) Operatør af en væsentlig tjeneste: En offentlig eller privat enhed, som er etableret i Danmark, og som opfylder kriterierne i § 3, stk. 1.
- 2) Net- og informationssystem:
  - a) Et elektronisk kommunikationsnet i form af en 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 ved brug 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.

### Kapitel 2

#### *Operatører af væsentlige tjenester*

§ 3. En enhed betragtes som en operatør af en væsentlig tjeneste, hvis

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

Stk. 2. Operatører af væsentlige tjenester skal registrere sig hos sundhedsministeren.

Stk. 3. Sundhedsministeren fastsætter nærmere regler om kriterierne i stk. 1 og registreringsordningen efter stk. 2.

### Kapitel 3

#### *Sikkerhedskrav*

§ 4. Operatører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som de anvender til deres aktiviteter, og med disse foranstaltninger sikre et sikkerhedsniveau, der er passende 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 sådanne væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester.

Stk. 3. Sundhedsministeren fastsætter nærmere regler om foranstaltningerne i stk. 1 og 2.

<sup>1)</sup> 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.

## Kapitel 4

### *Underretningspligt m.v.*

§ 5. Operatører af væsentlige tjenester skal hurtigst muligt underrette sundhedsministeren og Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Underretningen skal indeholde oplysninger, der gør det muligt for sundhedsministeren at fastslå 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.* Tillader omstændighederne det, meddeler sundhedsministeren relevante oplysninger til den underrettende operatør af en væsentlig tjeneste om opfølgningen på dennes underretning, herunder oplysninger der kan støtte en effektiv håndtering af hændelsen.

*Stk. 4.* Sundhedsministeren kan efter høring af den underrettende operatør af en væsentlig tjeneste oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

*Stk. 5.* Sundhedsministeren fastsætter nærmere regler om underretning efter stk. 1, herunder hvilke oplysninger der skal underrettes om, og kriterierne for fastlæggelsen af omfanget af en hændelses konsekvenser efter stk. 2.

§ 6. Sundhedsministeren kan fastsætte regler om, at skriftlig kommunikation til og fra sundhedsministeren om nærmere bestemte forhold, som er omfattet af denne lov eller af regler udstedt i medfør af loven, skal foregå digitalt.

*Stk. 2.* En digital meddelelse anses for at være kommet rettidigt frem, når den er tilgængelig for adressaten for meddelelsen.

*Stk. 3.* Sundhedsministeren kan fastsætte regler om digital kommunikation, herunder om anvendelse af bestemte it-systemer, særlige digitale formater og digital signatur el.lign.

## Kapitel 5

### *Tilsyn og påbud*

§ 7. Sundhedsministeren fører tilsyn med de forpligtelser, der påhviler operatører af væsentlige tjenester i henhold til denne lov og regler, der er udstedt i medfør af loven.

*Stk. 2.* Sundhedsministeren kan som led i sit tilsyn kræve, at operatører af væsentlige tjenester stiller oplysninger, der er nødvendige for tilsynet, til rådighed, herunder oplysninger der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer og dokumentation for den faktiske gennemførelse af sikkerhedspolitikker.

§ 8. Sundhedsministeren kan påbyde operatører af væsentlige tjenester at efterkomme forpligtelser i henhold til denne lov og regler, der er udstedt i medfør af loven.

## Kapitel 6

### *Delegation af beføjelser til Sundhedsdatastyrelsen*

§ 9. Sundhedsministeren kan bemyndige Sundhedsdatastyrelsen til at varetage opgaver, der i denne lov er tillagt ministeren.

## Kapitel 7

### *Straf*

§ 10. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde den, der undlader at efterkomme sundhedsministerens påbud efter § 8.

*Stk. 2.* I regler, der fastsættes i medfør af loven, kan der fastsættes straf i form af bøde.

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

## Kapitel 8

### *Ikrafttræden m.v.*

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

§ 12. Loven gælder ikke for Færøerne og Grønland.

## Bemærkninger til lovforslaget

### Almindelige bemærkninger

#### 1. Indledning

Lovforslaget har til formål at implementere 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 (herefter NIS-direktivet) inden for sundhedssektoren.

Den øgede digitalisering af det danske samfund indebærer, at net- og informationssikkerhed spiller en mere afgørende rolle. Dette gælder 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 sikkerheds-hændelser 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 f.eks. være et cyberangreb eller en oversvømmelse af et serverrum, der hindrer tjenester i at fungere, hæmmer en hensigtsmæssig behandling og pleje samt truer patientsikkerheden. Sikkerhedshændelser kan dermed underminere borgernes tillid til sundhedsvæsenet.

Det følger af NIS-direktivet, at tjenester, der leveres til sundhedssektoren, kan være af særlig samfundskritisk karakter. NIS-direktivet har derfor bl.a. til formål at sikre et højt niveau af net- og informationssikkerhed inden for sundhedssektoren, herunder sygehuse, praksissektoren, kommunal pleje m.v.

Ved gennemførelse af NIS-direktivets sikkerheds- og underretningskrav sikres der således i højere grad en beskyttelse af net- og informationssystemer inden for sundhedssektoren med det formål at opretholde driften af et funktionelt sundhedsvæsen, herunder bl.a. behandling og pleje af patienter og borgere.

Implementering af NIS-direktivet i dansk ret inden for sundhedssektoren forudsætter, at der vedtages ny lovgivning, der gør det muligt at fastsætte krav til sikkerhed og underretning for at sikre et højt sikkerhedsniveau for net- og informationssystemer inden for sundhedssektoren. Ifølge NIS-direktivet skal loven træde i kraft den 10. maj 2018.

#### 2. Gældende ret

Der findes ikke en generel og tværgående regulering af krav til sikkerhed og underretning for net- og informationssystemer inden for sundhedssektoren.

Den offentlige og private sektor er – indtil den 24. maj 2018 – omfattet af lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer (herefter persondataloven) og tilhørende bekendtgørelser, når der behandles personoplysninger. Det fremgår bl.a. af persondata-

loven, at der skal træffes fornødne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandling af personoplysninger. Persondataloven gennemfører Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter databeskyttelsesdirektivet). For så vidt angår den offentlige forvaltning finder bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning med senere ændringer anvendelse (herefter sikkerhedsbekendtgørelsen).

Databeskyttelsesdirektivet ophæves den 25. maj 2018, jf. Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (herefter databeskyttelsesforordningen), som finder anvendelse fra den 25. maj 2018.

Justitsministeren har den 25. oktober 2017 fremsat lovforslag L 68 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter forslag til databeskyttelsesloven). I forslag til databeskyttelsesloven, der fastsætter supplerende nationale bestemmelser om behandling af personoplysninger, foreslås det bl.a., at persondataloven ophæves, jf. forslaget § 46, stk. 2. I den forbindelse foreslås sikkerhedsbekendtgørelsen samtidig ophævet.

Efter den 25. maj 2018 vil det være reglerne i databeskyttelsesforordningen, suppleret af lovforslag til databeskyttelsesloven, lov om retshåndhævende myndigheders behandling af personoplysninger samt diverse særregler, herunder bl.a. regler i sundhedsloven m.v., der regulerer området for behandling af personoplysninger.

Derudover følger det af § 28, stk. 1, i lovbekendtgørelse nr. 433 af 22. april 2014 (herefter forvaltningsloven), at en forvaltningsmyndighed skal overholde reglerne i persondataloven, når der videregives personoplysninger til en anden forvaltningsmyndighed. Ifølge lovforslag L 69 til L 68, som blev behandlet samlet, er der sket en tilpasning af forvaltningslovens § 28, så der fremover henvises til reglerne i databeskyttelsesforordningen og forslag til databeskyttelsesloven. Desuden fremgår det af forvaltningslovens § 28, stk. 2, at oplysninger af fortrolig karakter, som ikke er personoplysninger, kun må videregives til en anden forvaltningsmyndighed, når den oplysningen angår udtrykkeligt har givet samtykke, når det følger af lov, eller bestemmelser fastsat i henhold til lov, at oplysningen skal videregives, eller det må antages, at oplysningen vil være af væsentlig betydning for myndighedens virksomhed eller for en afgørelse, myndigheden skal træffe. En oplysning anses som fortrolig, hvis den er af en sådan karakter, at den efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighe-

dens kendskab. Forvaltningsloven indeholder ikke bestemmelser om adgang til udveksling af ikke-fortrolige oplysninger, og sådanne oplysninger vil som udgangspunkt frit kunne videregives til en anden forvaltningsmyndighed.

Det følger derudover af forvaltningslovens § 27, stk. 1, at den, der virker inden for den offentlige forvaltning, har tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, med hensyn til en række oplysninger.

Straffeloven indeholder ikke i øvrigt nogen nærmere angivelse af, hvilke offentlige eller private interesser der kan føre til, at en oplysning må anses for at være fortrolig. En sådan angivelse findes derimod i forvaltningslovens § 27, hvor der er foretaget en opregning af hensyn, som efter en konkret vurdering i hvert enkelt tilfælde kan føre til, at en oplysning er fortrolig og dermed undergivet tavshedspligt. Opregningen er ikke udtømmende, men den må antages at dække langt den overvejende del af de hensyn, der kan føre til tavshedspligt med hensyn til oplysninger om juridiske personer. I forhold til tavshedspligt med oplysninger om fysiske personer udfyldes og suppleres bestemmelserne i forvaltningslovens § 27 med de centrale bestemmelser i persondataloven.

Det bemærkes endvidere, at forvaltningsmyndigheder i deres virke skal overholde god forvaltningsskik, og at de skal agere inden for de rammer, der kan udledes af de almindelige forvaltningsretlige grundsætninger om proportionalitet og saglighed i forvaltningen. Dette gælder også ved forvaltningsmyndigheders offentliggørelse af oplysninger.

Endelig bemærkes det, at i tilfælde af forvaltningsmyndigheders anvendelse af tvangsindgreb og oplysningspligter uden for strafferetsplejen, f.eks. i tilfælde af kontrol- og tilsynsbesøg, finder lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter med senere ændringer (herefter retssikkerhedsloven) anvendelse, således at denne lovs processuelle regler skal afholdes ved gennemførelsen af tilsynet.

### **3. 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 (NIS-direktivet)**

NIS-direktivet har til formål at sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i Unionen for at forbedre det indre markeds funktion.

NIS-direktivet fastsætter forpligtelser for alle medlemsstater til at vedtage en national strategi for sikkerhed i net- og informationssystemer. I medfør af NIS-direktivet skal der oprettes en samarbejdsgruppe med henblik på at støtte og lette strategisk samarbejde og udveksling af oplysninger mellem medlemsstaterne samt skabe tillid blandt dem. Endvidere skal der i medfør af NIS-direktivet oprettes et netværk af enheder, der håndterer IT-sikkerhedshændelser (CSIRT-netværk) med henblik på at bidrage til skabelsen af tillid mellem medlemsstaterne og at fremme et hurtigt og effektivt operationelt samarbejde. Yderligere fastsætter direktivet sikkerhedskrav og en underretningspligt for operatører

af væsentlige tjenester og for udbydere af digitale tjenester. Endelig fastsætter direktivet forpligtelser for medlemsstaterne til at udpege nationale kompetente myndigheder, centrale kontaktpunkter og CSIRT'er, som pålægges opgaver relateret til sikkerheden i net- og informationssystemer.

Det følger af NIS-direktivet, at behandling af personoplysninger udføres i overensstemmelse med databeskyttelsesdirektivet.

NIS-direktivet er et minimumsdirektiv, hvorfor medlemsstaterne kan vedtage eller bibeholde bestemmelser, som har til formål at nå et højere sikkerhedsniveau for net- og informationssystemer.

#### *3.1. Implementering af NIS-direktivet i dansk ret*

NIS-direktivet er et sektorspecifikt direktiv.

Det følger af NIS-direktivet, at hver medlemsstat udpeger en eller flere nationale kompetente myndigheder for sikkerheden i net- og informationssystemer inden for energi-, transport-, bank-, finans- og sundhedssektoren.

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.

NIS-direktivet har et bredt anvendelsesområde, men forudsætningen for en målrettet og erhvervsvenlig direktivimplementering, hvor danske virksomheder 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 sikkerhed for net- og informationssystemer.

Derudover er det vurderet hensigtsmæssigt, at Center for Cybersikkerhed varetager funktionen som henholdsvis nationalt centralt kontaktpunkt og Computer Security Incident Response Team (herefter CSIRT). Disse funktioner indebærer bl.a. 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 og fremme anvendelsen af fælles eller standardiserede systemer til klassificering af hændelser, risici og oplysninger.

Følgende afsnit gennemgår NIS-direktivets artikler, der er relevante for implementeringen af direktivet på Sundheds- og Ældreministeriets område.

#### *3.2. 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 tjene-

ster skal det indgå, om en enhed leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige 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.

### 3.3. Sikkerhedskrav for operatører af væsentlige tjenester

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 er passende 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 væsentlige tjenester.

### 3.4. Underretningspligt for operatører af væsentlige tjenester og offentliggørelse af hændelser

Ifølge NIS-direktivet skal medlemsstaterne sikre, at operatører af væsentlige tjenester hurtigst muligt foretager en underretning til den kompetente myndighed eller CSIRT om hændelser, der har væsentlige konsekvenser for kontinuiteten af deres væsentlige tjenester. Underretningen skal indeholde oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. Vurderes hændelsen at have konsekvenser for kontinuiteten af væsentlige tjenester i andre medlemsstater oplyser den kompetente myndighed eller CSIRT den eller de øvrige 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 patienter under operatørens pleje pr. år.

I henhold til NIS-direktivet kan den kompetente myndighed eller CSIRT efter høring af operatøren af den væsentlige tjeneste 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 kommercielle interesser.

### 3.5. Tilsyn og påbud

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 er 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 påviste mangler, kan den kompetente myndighed udstede påbud til operatører af væsentlige tjenester efter myndighedens vurdering af de indhentede oplysninger.

## 4. Sundheds- og Ældreministeriets overvejelser og den foreslåede ordning

Lovforslaget er et udtryk for en direktivnær implementering af NIS-direktivet. I 2015 besluttede regeringen fem principper for implementering af EU-regulering, som har til formål at sikre, at ny EU-regulering ikke overimplementeres, medmindre væsentlige hensyn taler herfor. Et af principperne fastsætter, at den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen. Derfor stilles der med lovforslaget ikke strengere krav til sikkerhed og underretning for operatører af væsentlige tjenester, end NIS-direktivet foreskriver.

Lovforslaget har til formål at øge beskyttelsen af net- og informationssystemer inden for sundhedssektoren med det formål at kunne opretholde driften af et funktionelt sundhedsvæsen, herunder behandling og pleje af patienter og borgere. Lovforslaget regulerer således ikke behandling af personoplysninger. Det fremgår i den forbindelse af NIS-direktivets artikel 2, stk. 1, at behandling af personoplysninger i henhold til NIS-direktivet udføres i overensstemmelse med databeskyttelsesdirektivet.

### 4.1. Identificering af operatører af væsentlige tjenester

Det foreslås, at der i lovforslaget indsættes bestemmelser om lovens anvendelsesområde og definitioner af lovens centrale begreber. De foreslåede definitioner af lovens centrale begreber implementerer NIS-direktivets artikel 4, nr. 1, 2, 4 og 7.

Ifølge lovforslaget skal en offentlig eller privat enhed, som er etableret i Danmark, betragtes som en operatør af en væsentlig tjeneste, hvis den pågældende enhed for det første leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter inden for sundhedssektoren. For det andet skal den tjeneste, som enheden leverer, afhænge af net- og informationssystemer. Endelig er det et krav, at en hændelse vil få væsentlige forstyrrende virkninger for leveringen af pågældende enheds tjeneste. Den foreslåede ordning om identificering af opera-

tører af væsentlige tjenester implementerer NIS-direktivets artikel 5, stk. 2, litra a-c.

Med henblik på at understøtte identificeringen af operatører af væsentlige tjenester foreslås det, at operatører af væsentlige tjenester skal lade sig registrere hos sundhedsministeren.

Det bemærkes, at en ikke-registreret enhed, som opfylder lovforslagets kriterier for at være en operatør af en væsentlig tjeneste, vil være underlagt lovforslagets forpligtelser.

Endelig foreslås det, at sundhedsministeren fastsætter nærmere regler om kriterierne for identificering af operatører af væsentlige tjenester og registreringsordningen.

#### 4.2. Sikkerhedskrav for operatører af væsentlige tjenester

Det følger af NIS-direktivet, at operatører af væsentlige tjenester skal træffe risikobaserede sikkerhedsforanstaltninger.

Det foreslås derfor, at operatører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som anvendes til deres aktiviteter med henblik på at sikre et sikkerhedsniveau, der er passende til risikoen. Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 1.

Det foreslås endvidere, at operatører af væsentlige tjenester skal træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i deres net- og informationssystemer med henblik på at sikre kontinuiteten i operatørernes væsentlige tjenester. Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 2.

Sundheds- og Ældreministeriet har vurderet det hensigtsmæssigt, at operatører af væsentlige tjenester kun underlægges proportionale krav, der ikke er unødvendigt byrdefulde. Med den foreslåede ordning overlades operatører af væsentlige tjenester derfor et skøn med hensyn til selv at bestemme indholdet af deres risikostyringsforanstaltninger under hensyntagen til de risici, som operatørerne er udsat for, det aktuelle trusselsbillede og teknologiens aktuelle stade.

Ifølge cyber- og informationssikkerhedsstrategien 2015-16 skal den internationale standard for informationsikkerhed, ISO27001, være implementeret af statslige myndigheder primo 2016. Derudover fremgår det af Den fælles-offentlige digitaliseringsstrategi 2016-2020, at regioner og kommuner skal følge principperne i ISO27001.

Sundheds- og Ældreministeriet har vurderet, at ISO27001-standarden er i overensstemmelse med NIS-direktivets formål, hvorfor den foreslåede ordning medfører mindre forpligtelser for myndigheder og de private aktører, der følger ISO27001-standarden.

Endelig foreslås det, at sundhedsministeren fastsætter nærmere regler om sikkerhedsforanstaltninger.

Det bemærkes, at de med lovforslaget foreslåede sikkerhedskrav vil finde anvendelse, uanset om der behandles personoplysninger i de pågældende net- og informationssystemer.

I det omfang der behandles personoplysninger, vil sikkerhedskravene i den til enhver tid gældende lovgivning om behandling af personoplysninger i øvrigt skulle følges.

#### 4.3. Underretningspligt for operatører af væsentlige tjenester og offentliggørelse af hændelser

Det følger af NIS-direktivet, at en operatør af en væsentlig tjeneste skal underrette den kompetente myndighed eller CSIRT i tilfælde af en hændelse, der har væsentlige konsekvenser for kontinuiteten af den væsentlige tjeneste.

Sundheds- og Ældreministeriet har vurderet det hensigtsmæssigt, at der sker en parallel underretning til henholdsvis sundhedsministeren og Center for Cybersikkerhed. På denne måde vil sundhedsministeren og Center for Cybersikkerhed få mulighed for hurtigt at reagere på en hændelse af grænseoverskridende karakter.

Derfor foreslås det, at operatører af væsentlige tjenester skal underrette sundhedsministeren og Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som de leverer. Operatøren af en væsentlig tjeneste skal foretage denne underretning hurtigst muligt. Underretningen vil skulle indeholde oplysninger, der gør det muligt for sundhedsministeren at klarlægge eventuelle grænseoverskridende konsekvenser af hændelsen. Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 3.

Med henblik på at fastlægge om en hændelse har væsentlige konsekvenser for kontinuiteten af en væsentlig tjeneste, foreslås det, at operatøren skal inddrage forhold som 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. Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 4, litra a-c.

For at understøtte en effektiv håndtering af hændelsen foreslås det, at sundhedsministeren meddeler relevante oplysninger til den underrettende operatør om opfølgningen på dennes underretning, hvis omstændighederne tillader det. Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 5.

Yderligere foreslås det, at sundhedsministeren – efter hørning af den underrettende operatør – kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse. Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 6.

Ved oplysning af offentligheden skal forstås, at sundhedsministeren kan gøre oplysningerne tilgængelige for en ubestemt kreds af modtagere, herunder f.eks. på en hjemmeside.

Det bemærkes, at sundhedsministeren ved oplysning af offentligheden skal overholde god forvaltningsskik, og at ministeren skal agere inden for de rammer, der kan udledes af de almindelige forvaltningsretlige grundsætninger om proportionalitet og saglighed i forvaltningen.

Såfremt den pågældende oplysning af offentligheden indebærer oplysning af personoplysninger, vil oplysningen bl.a.

skulle overholde reglerne i databeskyttelsesforordningen, forslag til databeskyttelsesloven og lov om retshåndhævende myndigheders behandling af personoplysninger.

Endelig foreslås det, at sundhedsministeren fastsætter nærmere regler om underretning og kriterierne for fastlæggelsen af omfanget af en hændelses konsekvenser.

#### 4.4. Digital kommunikation

Sundheds- og Ældreministeriet har vurderet det hensigtsmæssigt at etablere den nødvendige hjemmel til at kunne pålægge operatører af væsentlige tjenester at anvende digital kommunikation gennem en fællesoffentlig indberetningsløsning på tværs af sektorerne til brug for operatører af væsentlige tjenesters underretning af hændelser.

Det foreslås, at sundhedsministeren bemyndiges til at kunne fastsætte regler om, at skriftlig kommunikation skal foregå digitalt. Det er hensigten, at udmøntningen af denne bestemmelse vil skulle understøtte den førnævnte fællesoffentlige indberetningsløsning, der vil skulle udvikles og anvendes på tværs af sektorerne. En digital meddelelse vil skulle anses for at være kommet frem, når den er tilgængelig for adressaten.

Endelig foreslås det, at sundhedsministeren kan fastsætte regler om digital kommunikation, herunder hvilke it-systemer og digitale formater der skal anvendes.

#### 4.5. Tilsyn og påbud

Det foreslås, at sundhedsministeren fører tilsyn med de forpligtelser, der påhviler operatører af væsentlige tjenester i henhold til loven og regler udstedt i medfør af loven. Sundhedsministeren vil som led i sit tilsyn kunne kræve, at operatører af væsentlige tjenester stiller oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker, og dokumentation for den faktiske gennemførelse af sikkerhedspolitikker til rådighed. Den foreslåede ordning implementerer NIS-direktivets artikel 15, stk. 2, litra a-b.

Det forventes, at sundhedsministeren vil kunne gennemføre sit tilsyn fysisk såvel som skriftligt. Ved fysiske tilsyn vil sundhedsministeren skulle udføre sit tilsyn i overensstemmelse med retssikkerhedsloven, således at denne lovs processuelle regler skal afholdes ved gennemførelsen af tilsynet, herunder bl.a. retssikkerhedslovens § 5 om underretning og § 10 om retten til ikke at inkriminere sig selv m.v.

Desuden foreslås det, at sundhedsministeren kan påbyde operatører af væsentlige tjenester at efterkomme forpligtelser i henhold til denne lov og regler, der er udstedt i medfør af loven. Den foreslåede ordning implementerer NIS-direktivets artikel 15, stk. 3.

Det bemærkes, at hvis der sker behandling af personoplysninger, er Datatilsynet tilsynsmyndighed.

#### 4.6. Delegation til Sundhedsdatastyrelsen

Det foreslås, at sundhedsministeren kan bemyndige Sundhedsdatastyrelsen til at varetage opgaver, der efter denne lov er tillagt ministeren.

Sundheds- og Ældreministeriet har vurderet det hensigtsmæssigt, at sundhedsministeren bemyndiger Sundhedsdatastyrelsen til at varetage opgaver, der i denne lov er tillagt ministeren, da styrelsen i forvejen har opgaver vedrørende bl.a. digitalisering, sundhedsdata og it-arkitektur i sundhedsvæsenet, herunder opgaver vedrørende informationsikkerhed.

Det betyder, at Sundhedsdatastyrelsen vil skulle varetage de opgaver, der efter denne lov er tillagt ministeren.

I det omfang Sundhedsdatastyrelsen selv er en operatør af en væsentlig tjeneste, vil sundhedsministeren dog selv skulle varetage de opgaver, der i denne lov er tillagt ministeren, herunder bl.a. føre tilsyn med Sundhedsdatastyrelsen.

#### 4.7. Videregivelse af oplysninger til andre myndigheder

Sundheds- og Ældreministeriet har vurderet, at sundhedsministeren vil kunne få behov for – i forbindelse med sikkerhedshændelser – at videregive fortrolige oplysninger til andre myndigheder, f.eks. Center for Cybersikkerhed der varetager funktionen som CSIRT.

Der eksisterer ikke i gældende ret en specifik regulering af videregivelse af oplysninger på tværs af sektorer i forbindelse med underretninger om hændelser fra operatører af væsentlige tjenester. Det vurderes dog, at videregivelsen af oplysninger til andre myndigheder kan ske inden for rammerne af gældende ret som anført i afsnit 2.

Videregivelse af fortrolige oplysninger skal ske på baggrund af en konkret vurdering af, om videregivelsen er af væsentlig betydning for, at sundhedsministeren kan varetage de opgaver, som er tillagt ministeren i henhold til denne lov, herunder for en afgørelse som ministeren skal træffe.

Sundhedsministeren skal i tilfælde af videregivelse af fortrolige oplysninger konkret vurdere, om betingelserne for videregivelse er opfyldt i det enkelte tilfælde.

Det bemærkes, at lovforslaget ikke regulerer videregivelse af personoplysninger. Såfremt sundhedsministeren vil få behov for at videregive personoplysninger, skal videregivelsen ske i overensstemmelse med gældende ret, herunder reglerne i databeskyttelsesforordningen, forslag til databeskyttelsesloven, lov om retshåndhævende myndigheders behandling af personoplysninger og forvaltningsloven.

#### 4.8. Straf

Det følger af NIS-direktivet, at der skal fastsættes regler om sanktioner, der skal anvendes i de tilfælde, hvor der sker overtrædelse af regler, der er vedtaget i medfør af direktivet. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning.

Det foreslås på den baggrund, at den der underlader at efterkomme sundhedsministerens påbud straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås endvidere, at der i regler, der fastsættes i medfør af loven kan fastsættes straf i form af bøde.

Endelig foreslås det, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Der henvises i øvrigt til bemærkningerne til lovforslaget §§ 8 og 10.

## 5. Økonomiske og administrative konsekvenser for det offentlige

Stat, regioner og kommuner, der er operatører af væsentlige tjenester, skal underrette sundhedsministeren om hændelser, der har væsentlige konsekvenser for kontinuiteten af deres væsentlige tjenester samt lade sig registrere som operatører af væsentlige tjenester.

Lovforslaget vurderes ikke at medføre økonomiske og administrative konsekvenser af betydning for regioner og kommuner.

Sundhedsministeren 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 Center for Cybersikkerhed herom.

Lovforslaget vurderes at medføre, at sundhedsministeren vil skulle varetage nye opgaver, herunder bl.a. føre tilsyn med samt modtage underretninger om hændelser fra operatører af væsentlige tjenester.

## 6. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

De økonomiske konsekvenser for erhvervslivet m.v. vil afhænge af operatører af væsentlige tjenesters eksisterende sikkerhedsniveau. Det vurderes, at lovforslaget medfører ikke-væsentlige økonomiske konsekvenser for erhvervslivet.

For så vidt angår administrative konsekvenser vil operatører af væsentlige tjenester skulle lade sig registrere hos sundhedsministeren og underrette sundhedsministeren om hændelser, der har væsentlige konsekvenser for leveringen af de pågældende væsentlige tjenester. Operatører af væsentlige tjenester vil desuden, efter anmodning fra sundhedsministeren, skulle levere oplysninger til brug for ministerens tilsyn. Det vurderes, at lovforslaget vil medføre ikke-væsentlige administrative konsekvenser for erhvervslivet. Endelig vurderes det, at kun et begrænset antal virksomheder vil blive omfattet af den nye regulering.

## 7. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

## 8. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

## 9. Forholdet til EU-retten

Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, 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.

Lovforslaget er et udtryk for en direktivnær implementering af NIS-direktivet. I 2015 besluttede regeringen fem principper for implementering af EU-regulering, som har til formål at sikre, at ny EU-regulering ikke overimplementeres, medmindre væsentlige hensyn taler herfor. Et af principperne fastsætter, at den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen. Derfor stilles der med lovforslaget ikke strengere krav til sikkerhed og underretning for operatører af væsentlige tjenester, end NIS-direktivet foreskriver.

## 10. Hørte myndigheder og organisationer

Et udkast til lovforslag har i perioden fra 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, Data-tilsynet, 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, Psykolognævnet, 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.



## 11. Sammenfattende skema

	Positive konsekvenser/ mindredgifter (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	Det vurderes, at lovforslaget vil medføre ikke-væsentlige økonomiske konsekvenser for erhvervslivet.
Administrative konsekvenser for erhvervslivet	Ingen	Det vurderes, at lovforslaget vil medføre ikke-væsentlige administrative konsekvenser for erhvervslivet.
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 2016/1148/EU 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)	J A	NEJ  X

### Bemærkninger til lovforslagets enkelte bestemmelser

#### Til § 1

Det foreslås, at loven gælder for operatører, der leverer væsentlige tjenester inden for sundhedssektoren.

Den foreslåede ordning angiver lovens anvendelsesområde.

Ved sundhedssektoren skal bl.a. forstås institutioner og funktioner, der har til formål at fremme befolkningens sundhed samt at forebygge og behandle sygdom, lidelse og funktionsbegrænsning for den enkelte.

Behandling af personoplysninger i henhold til lovforslaget udføres i overensstemmelse med databeskyttelsesforordningen, forslag til databeskyttelsesloven og lov om retshåndhævende myndigheders behandling af personoplysninger.

#### Til § 2

Det foreslås at indsætte definitioner på en række af de centrale begreber, som anvendes i den foreslåede lov.

Med *nr. 1* defineres en operatør af en væsentlig tjeneste som en offentlig eller privat enhed, som er etableret i Danmark, og som opfylder kriterierne i § 3, stk. 1.

Denne definition svarer til definitionen i NIS-direktivets artikel 4, nr. 4.

Med *nr. 2* defineres net- og informationssystemer som a) et elektronisk kommunikationsnet i form af en 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 ved brug af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.

Denne definition svarer til definitionen i NIS-direktivets artikel 4, nr. 1.

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.

Denne definition svarer til definitionen i NIS-direktivets artikel 4, nr. 2.

Med *nr. 4* defineres en hændelse som enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.

Denne definition svarer til definitionen i NIS-direktivets artikel 4, nr. 7.

### *Til § 3*

#### Til stk. 1

I gældende ret findes der ikke nogen definition af begrebet operatør af en væsentlig tjeneste inden for sundhedssektoren.

Det foreslås, at en enhed betragtes som en operatør af en væsentlig tjeneste, hvis enheden leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter inden for sundhedssektoren, leveringen af denne tjeneste afhænger af net- og informationssystemer, og en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

Den foreslåede ordning implementerer NIS-direktivets artikel 5, stk. 2, litra a-c.

I vurderingen af, hvorvidt en hændelse vil få væsentlige forstyrrende virkninger for leveringen af en væsentlig tjeneste, vil faktorer som antallet af brugere, der er afhængige af tjenesten til private eller erhvervmæssige formål, herunder bl.a. antallet af patienter og borgere under operatørens virke pr. år, og hændelsens betydning for patientsikkerheden f.eks. kunne indgå.

#### Til stk. 2

Det foreslås, at operatører af væsentlige tjenester skal registrere sig hos sundhedsministeren.

Det er hensigten, at en operatør af en væsentlig tjeneste skal lade sig registrere via en hjemmeside.

En registrering vil ikke have betydning for, om en enhed er omfattet af lovforslagets definition og kriterier. Det betyder, at en ikke-registreret enhed, som opfylder lovforslagets kriterier for at være en operatør af en væsentlig tjeneste, vil være underlagt de forpligtelser, der følger af lovforslaget.

#### Til stk. 3

Det foreslås, at sundhedsministeren fastsætter nærmere regler om kriterierne i stk. 1 og registreringsordningen efter stk. 2.

Det er hensigten, at sundhedsministeren udsteder en bekendtgørelse, der præciserer kriterierne for at være en operatør af en væsentlig tjeneste.

Det forventes, at begrebet kritiske samfundsmæssige eller økonomiske aktiviteter inden for sundhedssektoren vil blive præciseret i bekendtgørelsen. Derudover forventes det, at det i bekendtgørelsen vil blive præciseret, hvilke momenter, der skal inddrages i vurderingen af, om en hændelse har væsentlige forstyrrende virkninger for leveringen af den væsentlige tjeneste.

Desuden forventes det, at der til bekendtgørelsen vil blive udarbejdet et bilag, som f.eks. angiver grænseværdier for, hvornår en hændelse vil få væsentlige forstyrrende virkninger for leveringen af en væsentlig tjeneste.

Det er endvidere hensigten, at sundhedsministeren ved bekendtgørelse vil fastsætte regler om registreringsordningen.

Det forventes, at der ved bekendtgørelse udstedes regler om de oplysninger, som en operatør af en væsentlig tjeneste skal meddele sundhedsministeren i forbindelse med registreringen, f.eks. kontaktoplysninger, oplysninger der er nødvendige for vurderingen af, om der leveres en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter inden for sundhedssektoren, oplysninger der er nødvendige for vurderingen af, om leveringen af tjenesten afhænger af net- og informationssystemer, oplysninger der er nødvendige for vurderingen af, om en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten samt oplysninger om, hvorvidt en operatør af en væsentlig tjeneste anvender en underleverandør.

Det bemærkes, at udmøntningen af bemyndigelsesbestemelsen vil skulle ske inden for rammerne af NIS-direktivet.

### *Til § 4*

#### Til stk. 1

Det foreslås, at operatører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som de anvender til deres aktiviteter og med disse foranstaltninger sikre et sikkerhedsniveau, der er passende til risikoen.

Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 1.

Det er hensigten, at de trufne sikkerhedsforanstaltninger så vidt muligt vil skulle basere sig på internationale sikkerhedsgodkendte standarder, f.eks. ISO27001.

Som eksempler på passende og forholdsmæssige tekniske og organisatoriske foranstaltninger kan bl.a. nævnes udarbejdelse af politikker og retningslinjer for net- og informationssikkerhed, etablering af intern organisering til styring af informationssikkerhed, sikring af medarbejderes bevidsthed om og efterlevelse af informationssikkerhed, udarbejdelse af retningslinjer for adgangsstyring og procedurer for brugeradgang, procedurer for hindring af uautoriseret adgang til net- og informationssystemer, foranstaltninger til beskyttelse mod malware, foranstaltninger til monitorering af hændelser og procedurer eller kontroller for gennemgang af informationssikkerhed.

Det er ikke hensigten, at operatører af væsentlige tjenester skal pålægges uforholdsmæssigt store økonomiske og administrative byrder. Under hensyntagen til teknologiens aktuelle stade vil sikkerhedsforanstaltningerne skulle være passende til den risiko, der er forbundet med leveringen af den pågældende væsentlige tjeneste.

Den foreslåede ordning skal ses i sammenhæng med den foreslåede bestemmelse i § 4, stk. 2. Begge bestemmelser

har til formål at fremme en risikostyringskultur, hvor der foretages risikovurderinger og gennemføres sikkerhedsforanstaltninger.

Til stk. 2

Det foreslås, at 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 sådanne væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester.

Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 2.

Som eksempler på passende foranstaltninger til at forebygge og minimere konsekvensen af hændelser kan bl.a. nævnes udarbejdelse af politikker og retningslinjer for net- og informationssikkerhed, sikring af medarbejderes bevidsthed om og efterlevelse af informationssikkerhed, procedurer for hindring af uautoriseret adgang til net- og informationssystemer, foranstaltninger til beskyttelse mod malware og foranstaltninger til monitorering af hændelser.

Det er ikke hensigten, at operatører af væsentlige tjenester skal pålægges uforholdsmæssigt store økonomiske og administrative byrder. Derfor vil foranstaltningerne skulle være passende til den risiko, der er forbundet med leveringen af den pågældende tjeneste.

Den foreslåede ordning skal ses i sammenhæng med den foreslåede bestemmelse i § 4, stk. 1. Begge bestemmelser har til formål at fremme en risikostyringskultur, hvor der foretages risikovurderinger og gennemføres sikkerhedsforanstaltninger.

Til stk. 3

Det foreslås, at sundhedsministeren fastsætter nærmere regler om foranstaltningerne i stk. 1 og 2.

Det er hensigten, at sundhedsministeren udsteder en bekendtgørelse, der nærmere præciserer mulige sikkerhedsforanstaltninger, f.eks. foranstaltninger der sikrer væsentlige tjenesters fortrolighed, integritet, tilgængelighed og robusthed.

Derudover er det hensigten, at bekendtgørelsen vil blive suppleret med en vejledning om sikkerhedsforanstaltninger til sikring af et højt sikkerhedsniveau i net- og informationssystemer.

Det bemærkes, at forpligtelsen til at træffe passende sikkerhedsforanstaltninger efter den foreslåede stk. 1 og stk. 2 vil gælde uanset udstedelsen af regler herom.

Det bemærkes endvidere, at såfremt der behandles personoplysninger, vil operatøren af en væsentlig tjeneste derudover skulle overholde de sikkerhedskrav, der følger af persondataloven og – for offentlige myndigheder – sikkerhedsbekendtgørelsen. Fra den 25. maj 2018, hvor databeskyttelsesforordningen finder anvendelse, vil en operatør af en væsentlig tjeneste, såfremt der behandles personoplysninger,

skulle overholde de sikkerhedskrav, der følger af forordningen.

Det bemærkes yderligere, at udmøntningen af bemyndigelsesbestemmelsen vil skulle ske inden for rammerne af NIS-direktivet.

## Til § 5

Til stk. 1

Det foreslås, at operatører af væsentlige tjenester hurtigst muligt skal underrette sundhedsministeren og Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Det foreslås endvidere, at underretningen skal indeholde oplysninger, der gør det muligt for sundhedsministeren at klarlægge eventuelle grænseoverskridende konsekvenser af hændelsen.

Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 3.

Det bemærkes, at Center for Cybersikkerhed varetager funktionen som CSIRT i Danmark. Der henvises i den forbindelse til bemærkningerne i afsnit 3.1.

Den foreslåede ordning betyder, at den pågældende operatør af en væsentlig tjeneste, under hensyntagen til arbejdet med at minimere konsekvenserne af hændelsen, vil skulle foretage en underretning til sundhedsministeren, så snart operatøren har erkendt, at hændelsen har væsentlige konsekvenser for kontinuiteten af den væsentlige tjeneste, der leveres.

Den foreslåede ordning betyder endvidere, at underretningen til sundhedsministeren bl.a. vil skulle indeholde oplysninger, der gør ministeren i stand til at vurdere, om hændelsen har konsekvenser for andre medlemslande. Det vil f.eks. være oplysninger om den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.

Det bemærkes, at operatører af væsentlige tjenester vil skulle være særligt opmærksomme på at få underrettet hurtigt i tilfælde af hændelser, der har grænseoverskridende konsekvenser.

Derudover bemærkes det, at såfremt en operatør af en væsentlig tjeneste er afhængig af en udbyder af digitale tjenester, vil operatøren skulle underrette om en hændelse, der berører udbyderen, såfremt hændelsen har væsentlige konsekvenser for kontinuiteten af operatørens levering af den væsentlige tjeneste. Denne forpligtelse følger af NIS-direktivets artikel 16, stk. 5. Dermed sikres det, at sundhedsministeren får kendskab til hændelser og mangler i sikkerheden hos udbydere af digitale tjenester, der har en negativ indvirkning på en operatørs levering af sin væsentlige tjeneste.

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. Denne definition bygger på NIS-direktivets artikel 4, nr. 6, og 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.

Til stk. 2

Det foreslås, at operatøren af en væsentlig tjeneste navnlig skal tage følgende kriterier i betragtning med henblik på at fastlægge omfanget af en hændelses konsekvenser efter stk. 1: 1) Antallet af brugere, der berøres af afbrydelsen af den væsentlige tjeneste, 2) hændelsens varighed og 3) den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.

Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 4.

Ved antallet af brugere der berøres af afbrydelsen af den væsentlige tjeneste, kan det bl.a. inddrages, hvor mange borgere og sundhedspersoner, der er omfattet af den pågældende tjeneste. Herunder bør det inddrages, om de pågældende borgere og sundhedspersoner er afhængige af tjenesten, og om tjenesten kan opnås på anden vis. Særligt bør det inddrages, om hændelsen påvirker sundhedspersoners udlevering og indhentning af oplysninger til brug for pleje og behandling.

Med henblik på fastlæggelse af en hændelses varighed kan det bl.a. inddrages, om det er muligt at opretholde tjenesten i tilstrækkeligt omfang uden adgang til net- og informationssystemer. Derudover kan det inddrages, hvor lang tid der skønnes at kunne gå, før afbrydelsen af tjenesten vil have negative konsekvenser for opretholdelsen af et funktionelt sundhedsvæsen, herunder bl.a. behandling og pleje af patienter og borgere.

I forbindelse med vurderingen af den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen, kan det bl.a. inddrages, hvor stort et geografisk område den væsentlige tjeneste dækker.

Det bemærkes, at det er hensigten, at der skal foretages en samlet vurdering af ovenstående kriterier.

Til stk. 3

Det foreslås, at såfremt omstændighederne tillader det, meddeler sundhedsministeren relevante oplysninger til den underrettede operatør af en væsentlig tjeneste om opfølgningen på dennes underretning, herunder oplysninger der kan støtte en effektiv håndtering af hændelsen.

Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 5.

Det er hensigten med den foreslåede ordning at sikre, hvis omstændighederne tillader det, at en operatør af en væsentlig tjeneste får en tilbagemelding, der kan understøtte operatørens videre arbejde med at begrænse hændelsen.

Til stk. 4

Det foreslås, at sundhedsministeren efter høring af den underrettede operatør af en væsentlig tjeneste kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens

kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Den foreslåede ordning implementerer NIS-direktivets artikel 14, stk. 5.

Hensigten med den foreslåede ordning er, at sundhedsministeren, inden oplysning af offentligheden om en konkret hændelse, bl.a. vil kunne høre operatøren af en væsentlig tjeneste over sagens faktiske omstændigheder.

Den foreslåede ordning indebærer, at sundhedsministeren 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.

Det er hensigten, under hensyntagen til hændelsens karakter, at offentliggørelse f.eks. vil kunne ske på en hjemmeside eller i en pressemeddelelse.

Det bemærkes, at en beslutning om offentliggørelse af en hændelse ikke er en afgørelse i forvaltningslovens forstand, dog skal forvaltningsmyndigheder i deres virke overholde god forvaltningsskik og agere inden for de rammer, der kan udledes af de almindelige forvaltningsretlige grundsætninger om proportionalitet og saglighed i forvaltningen.

Såfremt der sker offentliggørelse af personoplysninger, vil offentliggørelsen derudover bl.a. skulle overholde reglerne i databeskyttelsesforordningen, forslag til databeskyttelsesloven og lov om retshåndhævende myndigheders behandling af personoplysninger.

Til stk. 5

Det foreslås, at sundhedsministeren fastsætter nærmere regler om underretning efter stk. 1, herunder hvilke oplysninger der skal underrettes om, og kriterierne for fastlæggelsen af omfanget af en hændelses konsekvenser efter stk. 2.

Det er hensigten, at sundhedsministeren udsteder en bekendtgørelse, der nærmere præciserer, hvilke oplysninger en underretning vil skulle indeholde, f.eks. kontaktoplysninger, oplysninger om konsekvenserne af hændelsen og de foranstaltninger, som operatøren af en væsentlig tjeneste har truffet eller vil træffe til afværgelse af hændelsen.

Endelig er det hensigten, at en operatør af en væsentlig tjeneste vil skulle foretage en underretning til sundhedsministeren, så snart operatøren har erkendt, at hændelsen har væsentlige konsekvenser for kontinuiteten af den væsentlige tjeneste, der leveres.

Det bemærkes, at i tilfælde af brud på persondatasikkerheden, vil der fra den 25. maj 2018, hvor databeskyttelsesforordningen finder anvendelse, skulle ske anmeldelse af brud på persondatasikkerheden til den relevante tilsynsmyndighed, dvs. Datatilsynet, uden unødigt forsinkelse og om muligt senest 72 timer efter at den dataansvarlige er blevet bekendt med bruddet, jf. forordningens artikel 33, stk. 1.

## Til § 6

### Til stk. 1

Det foreslås, at sundhedsministeren kan fastsætte regler om, at skriftlig kommunikation til og fra sundhedsministeren om nærmere bestemte forhold, som er omfattet af denne lov eller af regler udstedt i medfør af loven, skal foregå digitalt.

Hensigten med den foreslåede ordning er at sikre en let og tilgængelig indberetningsløsning.

En udmøntning af bemyndigelsesbestemmelsen vil pålægge operatører af væsentlige tjenester en pligt til at anvende en digital indberetningsløsning.

### Til stk. 2

Det foreslås, at en digital meddelelse anses for at være kommet frem, når den er tilgængelig for adressaten for meddelelsen.

En digital meddelelse anses for at være kommet rettidigt frem, hvis meddelelsen er kommet frem inden kontortids ophør.

Hensigten med den foreslåede ordning er at sikre en ensartet retsvirkning af afsendelse af digital kommunikation som med fysisk post.

Forslaget indebærer, at meddelelser til eller fra sundhedsministeren, der sendes på den foreskrevne digitale måde, anses for at være kommet frem til sundhedsministeren på det tidspunkt, hvor meddelelsen er tilgængelig digitalt for ministeren.

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 således 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 stk. 3

Det foreslås, at sundhedsministeren kan fastsætte regler om digital kommunikation, herunder om anvendelse af bestemte it-systemer, særlige digitale formater og digital signatur el.lign.

Den foreslåede bestemmelse indebærer, at det kan gøres obligatorisk for operatører af væsentlige tjenester at anvende bestemte internetløsninger, herunder selvbetjeningsløsninger.

Bestemmelsen indebærer endvidere, at skriftlige henvendelser til sundhedsministeren om forhold, som er omfattet af et krav om digital kommunikation, ikke anses for behørigt modtaget af sundhedsministeren, hvis de indsendes på anden vis end den foreskrevne digitale måde.

Hvis en operatør af en væsentlig tjeneste retter henvendelse til sundhedsministeren på anden måde end den foreskrevne digitale måde, eksempelvis ved brev, følger det af den al-

mindelige vejledningspligt, at sundhedsministeren skal vejlede om reglerne på området, herunder om pligten til at kommunikere digitalt.

Herudover indebærer bestemmelsen, at der kan fastsættes regler om, at en operatør af en væsentlig tjeneste, som retter henvendelse til sundhedsministeren, skal oplyse en e-mail-adresse, som operatøren kan kontaktes på i forbindelse med behandlingen af en konkret sag eller henvendelse til sundhedsministeren. I den forbindelse kan der også pålægges den pågældende operatør af en væsentlig tjeneste en pligt til at underrette sundhedsministeren 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.

Muligheden for at blive fritaget for pligten til digital kommunikation tænkes navnlig anvendt, hvor det er påkrævet at anvende en dansk digital signatur, men hvor der er tale om en operatør af en væsentlig tjeneste med hjemsted i udlandet, som 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 operatør af en væsentlig tjenestes computere ikke fungerer, at operatøren har mistet koden til sin digitale signatur, eller at der opstår lignende hindringer, som det er op til operatøren at overvinde, kan ikke føre til fritagelse for pligten til digital kommunikation. I så fald må den pågældende operatør af en væsentlig tjeneste eksempelvis anmode en rådgiver om at varetage kommunikationen på operatørens vegne.

## Til § 7

### Til stk. 1

Det foreslås, at sundhedsministeren fører tilsyn med de forpligtelser, der påhviler operatører af væsentlige tjenester i henhold til denne lov og regler, der er udstedt i medfør af loven.

Det er hensigten, at sundhedsministeren løbende vil kunne gennemføre tilsyn med udvalgte operatører af væsentlige tjenester. Sundhedsministeren vil kunne gennemføre et tilsyn af egen drift eller på baggrund af en underretning om en hændelse.

Det forventes, at sundhedsministeren kan gennemføre sit tilsyn fysisk såvel som skriftligt. Ved fysiske tilsyn vil sundhedsministeren skulle udføre sit tilsyn i overensstemmelse med retssikkerhedsloven, således at denne lovs processuelle regler skal afholdes ved gennemførelsen af tilsynet, herunder bl.a. retssikkerhedslovens § 5 om underretning og § 10 om retten til ikke at inkriminere sig selv m.v.

Det bemærkes, at hvis der sker behandling af personoplysninger, er Datatilsynet tilsynsmyndighed.

### Til stk. 2

Det foreslås, at sundhedsministeren som led i sit tilsyn kan kræve, at operatører af væsentlige tjenester stiller oplys-

ninger, der er nødvendige for tilsynet, til rådighed, herunder oplysninger der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer og dokumentation for den faktiske gennemførelse af sikkerhedspolitikker.

Som eksempel på oplysninger, der er nødvendige for at vurdere sikkerheden i net- og informationssystemer, kan nævnes risikovurderinger, den tilgrundliggende dokumentation for operatørens valg af de foretagne tekniske og organisatoriske foranstaltninger og en operatør af en væsentlig tjenestes sikkerheds- eller beredskabspolitik i tilfælde af hændelser, der vil få væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som operatøren leverer.

Som eksempel på dokumentation for den faktiske gennemførelse af sikkerhedspolitikker kan nævnes resultaterne af en sikkerhedsaudit, f.eks. resultaterne af en sikkerhedsaudit udført af en kvalificeret auditør.

Det bemærkes, at oplysninger og dokumentation skal forstås i vid forstand og omfatter bl.a. fysiske dokumenter og elektroniske oplysninger.

#### *Til § 8*

Det foreslås, at sundhedsministeren kan påbyde operatører af væsentlige tjenester at efterkomme forpligtelser i henhold til denne lov og regler, der er udstedt i medfør af loven.

Det betyder, at sundhedsministeren vil kunne udstede påbud om, at en operatør af en væsentlig tjeneste f.eks. skal afhjælpe en påvist mangel i operatørens tekniske eller organisatoriske sikkerhedsforanstaltninger, herunder f.eks. mangler i den risikovurdering, der ligger til grund for de valgte tekniske eller organisatoriske sikkerhedsforanstaltninger.

Det forventes, at sundhedsministeren særligt vil udstede påbud i tilfælde af manglende overholdelse af sikkerhedskravene anført i lovforslagets § 4.

Dog vil sundhedsministeren også kunne udstede påbud i tilfælde af, at operatører af væsentlige tjenester ikke efterkommer lovforslagets øvrige krav, f.eks. kravet om registrering og kravet om underretning i tilfælde hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som operatørerne leverer.

Sundhedsministeren vil kunne meddele henstillinger, forinden der meddeles påbud.

Udstedelse af påbud skal i øvrigt ske i overensstemmelse med de forvaltningsretlige regler, herunder bl.a. reglerne om partshøring, begrundelse og klagevejledning.

#### *Til § 9*

Det foreslås, at sundhedsministeren kan bemyndige Sundhedsdatastyrelsen til at varetage opgaver, der i denne lov er tillagt ministeren.

Sundheds- og Ældreministeriet har vurderet det hensigtsmæssigt, at sundhedsministeren bemyndiger Sundhedsdatastyrelsen til at varetage opgaver, der i lovforslaget er tillagt ministeren, da Sundhedsdatastyrelsen i forvejen har opgaver vedrørende bl.a. digitalisering, sundhedsdata og it-arkitektur

i sundhedsvæsenet, herunder opgaver vedrørende informationsikkerhed.

Dermed vil Sundhedsdatastyrelsen skulle varetage samtlige opgaver, som sundhedsministeren skal varetage i henhold til lovforslaget.

I det omfang Sundhedsdatastyrelsen selv er en operatør af en væsentlig tjeneste, vil sundhedsministeren dog selv skulle varetage de opgaver, der i lovforslaget er tillagt ministeren, herunder bl.a. føre tilsyn med Sundhedsdatastyrelsen.

#### *Til § 10*

Til stk. 1

Efter den foreslåede ordning skal den, der uagtsomt eller forsætteligt undlader at efterkomme sundhedsministerens påbud efter lovforslagets § 8, kunne straffes med bøde.

Bestemmelsen implementerer NIS-direktivets artikel 21, der bestemmer, at der skal fastættes sanktioner, der skal anvendes i tilfælde af overtrædelse af regler, der er vedtaget i medfør af direktivet.

Det betyder, at det gøres muligt at straffe overtrædelse af lovforslagets § 8, hvorefter sundhedsministeren kan påbyde operatører af væsentlige tjenester at efterkomme forpligtelser i henhold til loven og regler, der er udstedt i medfør af loven.

Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have en afskrækkende virkning.

Den foreslåede ordning vil bl.a. gøre det muligt at straffe manglende efterlevelse af påbud om at overholde sikkerhedskravene anført i den foreslåede bestemmelse i § 4, stk. 1, der fastsætter, at operatører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som anvendes til deres aktiviteter og med disse foranstaltninger sikre et sikkerhedsniveau, der er passende til risikoen.

Derudover vil lovforslaget gøre det muligt at straffe manglende efterlevelse af påbud om at overholde sikkerhedskravene anført i den foreslåede bestemmelse i § 4, stk. 2, der fastsætter, at 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 sådanne væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester.

Til stk. 2

Det foreslås, at der i regler, der fastsættes i medfør af loven, kan fastsætte straf i form af bøde.

Til stk. 3

Det foreslås, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

*Til § 11*

Det foreslås, at loven træder i kraft den 10. maj 2018.

Det foreslåede ikrafttrædelsestidspunkt følger af 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 endvidere 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 § 12*

Det foreslås, at loven ikke gælder for Færøerne og Grønland.

Baggrunden for den foreslåede ordning er, at Grønland har overtaget sundhedsvæsenet i Grønland, og Færøerne har overtaget de relevante dele af sundhedsområdet på Færøerne.

**Bilag 1****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**

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg,<sup>1)</sup>

efter den almindelige lovgivningsprocedure<sup>2)</sup>, og ud fra følgende betragtninger:

- (1) Net- og informationssystemer og net- og informationstjenester spiller en afgørende rolle i samfundet. Det er af afgørende betydning for de økonomiske og samfundsmæssige aktiviteter og navnlig for et velfungerende indre marked, at de er pålidelige og sikre.
- (2) Omfanget, hyppigheden og konsekvenserne af sikkerhedshændelser er tiltagende og udgør en alvorlig trussel for driften af net- og informationssystemer. Disse systemer kan endvidere blive et mål for forsætligt skadelige handlinger, som har til formål at ødelægge eller forstyrre systemernes drift. Sådanne hændelser kan hindre gennemførelsen af økonomiske aktiviteter, medføre betydelige finansielle tab, underminere brugernes tillid og forårsage stor skade på Unionens økonomi.
- (3) Net- og informationssystemer og navnlig internettet spiller en væsentlig rolle, når det gælder om at fremme grænseoverskridende bevægelighed for varer, tjenester og personer. På grund af den tværnationale karakter vil betydelige afbrydelser af sådanne systemer, hvad enten de er tilsigtede eller utilsigtede, og uanset hvor de opstår, kunne påvirke de enkelte medlemsstater og Unionen som helhed. Sikkerheden i net- og informationssystemer er derfor afgørende for et velfungerende indre marked.
- (4) Med udgangspunkt i de væsentlige fremskridt, der er gjort inden for det europæiske forum af medlemsstater med at fremme drøftelser og udvekslinger om god praksis for politikker, herunder udvikling af principper for et europæisk cyberkrisesamarbejde, bør der oprettes en samarbejdsgruppe bestående af repræsentanter for medlemsstaterne, Kommissionen og Den Europæiske Unions Agentur for Net- og Informationssikkerhed («ENISA») for at støtte og fremme et strategisk samarbejde mellem medlemsstaterne vedrørende sikkerhed for net- og informationssystemer. Hvis denne gruppe skal være effektiv og inklusiv, er det vigtigt, at alle medlemsstater har et minimum af kapacitet og en strategi, der sikrer et højt sikkerhedsniveau for net- og informationssystemer på medlemsstaternes område. Dertil kommer, at sikkerhedskrav og underretningspligt bør gælde for operatører af væsentlige tjenester og udbydere af digitale tjenester for at fremme en risikostyringskultur og sikre underretning om de mest alvorlige hændelser.
- (5) Den eksisterende kapacitet er ikke tilstrækkelig til at sikre et højt sikkerhedsniveau for net- og informationssystemer i Unionen. Medlemsstaterne har meget forskellige beredskabsniveauer, hvilket har ført til en usammenhængende tilgang i Unionen som helhed. Dette resulterer i et uensartet beskyttelsesniveau for forbrugere og virksomheder og undergraver det samlede sikkerhedsniveau for



net- og informationssystemer i Unionen. Manglende fælles krav til operatører af væsentlige tjenester og udbydere af digitale tjenester gør det også umuligt at iværksætte en overordnet og effektiv samarbejdsmechanisme på EU-plan. Universiteter og forskningscentre har en afgørende rolle at spille med hensyn til at fremme forskning, udvikling og innovation på disse områder.

- (6) En effektiv reaktion på de sikkerhedsproblemer, der opstår i net- og informationssystemer, forudsætter derfor en samlet tilgang på EU-plan med fælles mindstekrav til kapacitetsopbygning og planlægning, udveksling af oplysninger, samarbejde og fælles sikkerhedskrav for operatører af væsentlige tjenester og udbydere af digitale tjenester. Operatører af væsentlige tjenester og udbydere af digitale tjenester er dog ikke afskåret fra at indføre strengere sikkerhedsforanstaltninger end dem, der er fastsat i dette direktiv.
- (7) For at dække alle relevante hændelser og risici bør dette direktiv både finde anvendelse for operatører af væsentlige tjenester og udbydere af digitale tjenester. Forpligtelserne for operatører af væsentlige tjenester og udbydere af digitale tjenester bør dog hverken finde anvendelse for virksomheder, der udbyder offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, jf. Europa-Parlamentets og Rådets direktiv 2002/21/EF<sup>3)</sup>, idet disse er omfattet af de særlige sikkerheds- og integritetskrav, der er fastsat i nævnte direktiv, eller finde anvendelse for tillidstjenesteudbydere, jf. Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014<sup>4)</sup>, som er underlagt sikkerhedskravene i nævnte forordning.
- (8) Dette direktiv bør ikke være til hinder for, at hver medlemsstat kan træffe de nødvendige foranstaltninger for at sikre beskyttelsen af sine væsentlige sikkerhedsinteresser, opretholde den offentlige orden og sikkerhed samt tillade efterforskning, afsløring og retsforfølgelse af strafbare handlinger. I henhold til artikel 346 i traktaten om Den Europæiske Unions funktionsmåde (TEUF) er ingen medlemsstat forpligtet til at meddele oplysninger, hvis udbredelse efter dens opfattelse ville stride mod dens væsentlige sikkerhedsinteresser. I den forbindelse er Rådets afgørelse 2013/488/EU<sup>5)</sup> og hemmeligholdelsesaftaler eller uformelle hemmeligholdelsesaftaler, f.eks. Traffic Light Protocol, af betydning.
- (9) Visse sektorer i økonomien er allerede reguleret eller vil fremover blive reguleret af sektorspecifikke EU-retsakter, der indeholder bestemmelser om sikkerheden i net- og informationssystemer. Når de pågældende EU-retsakter indeholder bestemmelser om indførelse af krav vedrørende sikkerheden i net- og informationssystemer eller underretninger om hændelser, bør disse bestemmelser anvendes, hvis de indeholder krav, der i praksis mindst svarer til forpligtelserne i dette direktiv. Medlemsstaterne bør i så fald anvende bestemmelserne i sådanne sektorspecifikke EU-retsakter, herunder bestemmelser, der vedrører jurisdiktion, og bør ikke gennemføre identifikationsprocessen for operatører af væsentlige tjenester som defineret i dette direktiv. I den forbindelse bør medlemsstaterne sende Kommissionen oplysninger om anvendelsen af sådanne lex specialis-bestemmelser. Når det skal fastlægges, om de krav til sikkerheden i net- og informationssystemer og underretninger om hændelser, der er indeholdt i sektorspecifikke EU-retsakter, svarer til bestemmelserne i dette direktiv, bør der kun tages hensyn til bestemmelserne i relevante EU-retsakter og deres anvendelse i medlemsstaterne.
- (10) I søfartssektoren dækker sikkerhedskrav for rederier, skibe, havnefaciliteter, havne og skibstrafik-tjenester i medfør af EU-retsakter alle operationer, herunder radio- og telekommunikationssystemer, computersystemer og -net. En del af de obligatoriske procedurer, der skal følges, omfatter un-

derretning om alle hændelser og bør derfor betragtes som *lex specialis*, såfremt disse krav mindst svarer til de tilsvarende bestemmelser i dette direktiv.

- (11) Når medlemsstaterne identificerer operatører i søfartssektoren, bør de tage hensyn til eksisterende og fremtidige internationale kodekser og vejledninger udarbejdet af navnlig Den Internationale Søfartsorganisation for at give de enkelte maritime operatører en sammenhængende tilgang.
- (12) Regulering og tilsyn i banksektoren og sektoren for finansielle markedsinfrastrukturer er stærkt harmoniseret på EU-plan under anvendelse af primær og sekundær EU-ret og standarder, der er udviklet i samarbejde med de europæiske tilsynsmyndigheder. Inden for bankunionen er anvendelsen af og tilsynet med disse krav sikret af den fælles tilsynsmekanisme. For medlemsstater, der ikke deltager i bankunionen, sikres dette af de relevante banktilsynsmyndigheder i medlemsstaterne. På andre områder af reguleringen af den finansielle sektor sikrer Det Europæiske Finanstillsynssystem også en høj grad af sammenfald mellem og ensartethed i tilsynspraksis. Den Europæiske Værdipapir- og Markedstilsynsmyndighed fører også direkte tilsyn med visse enheder, nemlig kreditvurderingsbureauer og transaktionsregistre.
- (13) Operationel risiko er en afgørende del af tilsynsmæssig regulering og tilsyn inden for banksektoren og sektoren for finansielle markedsinfrastrukturer. Den omfatter alle operationer, herunder net- og informationssystemers sikkerhed, robusthed og integritet. Kravene vedrørende disse systemer, som ofte overstiger de krav, der er fastsat i dette direktiv, er fastsat i en række EU-retsakter, herunder regler om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber og om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber, der indeholder krav vedrørende operationel risiko, regler om markeder for finansielle instrumenter, der indeholder krav vedrørende risikovurdering for investeringsselskaber og for regulerede markeder, regler om OTC-derivater, centrale modparter og transaktionsregistre, der indeholder krav vedrørende operationel risiko for centrale modparter og transaktionsregistre, og regler om forbedring af værdipapirafviklingen i Unionen og om værdipapircentraler, der indeholder krav vedrørende operationel risiko. Desuden indgår krav om underretning om hændelser i normal tilsynspraksis i den finansielle sektor og findes ofte i tilsynsmanualer. Medlemsstaterne bør tage hensyn til disse regler og krav ved anvendelse af *lex specialis*.
- (14) Som Den Europæiske Centralbank bemærker i sin udtalelse af 25. juli 2014<sup>6)</sup>, berører dette direktiv ikke regimet i henhold til EU-retten for Eurosystemets overvågning af betalings- og afviklingssystemer. Det vil være passende, hvis de myndigheder, der er ansvarlige for den pågældende overvågning, udveksler erfaringer om forhold vedrørende sikkerhed i net- og informationssystemer med de kompetente myndigheder efter dette direktiv. Det samme hensyn gælder medlemmer uden for euroområdet af Det Europæiske System af Centralbanker, der foretager en sådan overvågning af betalings- og afviklingssystemer på grundlag af nationale love og bestemmelser.
- (15) En onlinemarkedsplads giver forbrugere og erhvervsdrivende mulighed for at indgå aftaler om køb eller tjenester online med erhvervsdrivende, og den er det endelige bestemmelsessted for indgåelse af sådanne kontrakter. Den bør ikke omfatte onlinetjenester, der kun tjener til at formidle tredjepartstjenester, hvor en kontrakt kan indgås i sidste ende. Den bør derfor ikke omfatte onlinetjenester, der sammenligner prisen på bestemte varer eller tjenester fra forskellige erhvervsdrivende og derefter omdirigerer brugeren til den foretrukne erhvervsdrivende for at købe produktet. Computing-tjenester leveret af onlinemarkedspladsen kan omfatte behandling af transaktioner, aggregering af data eller analyse af brugere. App-butikker, der fungerer som onlineforretninger med henblik på digital

distribution af applikationer eller softwareprogrammer fra tredjemand, anses som værende en form for onlinemarkedsplads.

- (16) En onlinesøgemaskine gør det principielt muligt for brugeren at foretage søgninger på alle websteder på grundlag af en forespørgsel om et hvilket som helst emne. Søgningen kan alternativt være fokuseret på websteder på et bestemt sprog. Definitionen af en onlinesøgemaskine, der er omhandlet i dette direktiv, bør ikke dække søgefunktioner, der er begrænset til indholdet af et særligt websted, uanset om søgefunktionen er fra en ekstern søgemaskine. Den bør heller ikke omfatte online-tjenester, der sammenligner prisen på bestemte varer eller tjenester fra forskellige erhvervsdrivende og derefter omdirigerer brugeren til den foretrukne erhvervsdrivende for at købe produktet.
- (17) Cloud computing-tjenester omfatter en lang række aktiviteter, der kan leveres i henhold til forskellige modeller. Med henblik på dette direktiv dækker udtrykket »cloud computing-tjenester« tjenester, som muliggør adgang til en skalerbar og elastisk pulje af delbare IT-ressourcer. Disse IT-ressourcer omfatter ressourcer som f.eks. netværk, servere eller anden infrastruktur, lagring, applikationer og tjenester. Udtrykket »skalerbar« henviser til IT-ressourcer, som kan tildeles fleksibelt af udbyderen af cloud computing-tjenester uanset ressourcernes geografiske placering med henblik på at håndtere udsving i efterspørgslen. Udtrykket »elastisk pulje« bruges til at beskrive de IT-ressourcer, der tilvejebringes og stilles til rådighed alt efter efterspørgslen for hurtigt at øge eller mindske de tilgængelige ressourcer alt efter arbejdsbyrden. Udtrykket »delbar« bruges til at beskrive de IT-ressourcer, der leveres til flere brugere, som deler en fælles adgang til tjenesten, men hvor databehandlingen foretages særskilt for hver bruger, selv om tjenesten leveres fra samme elektroniske udstyr.
- (18) Et internetudvekslingspunkt (IXP) har som funktion at sammenkoble net. Et IXP giver ikke netadgang og fungerer ikke som transitleverandør eller -operatør. Et IXP leverer heller ikke andre tjenester, som ikke er forbundet med samtrafik, selv om dette ikke forhindrer en IXP-operatør i at levere ikkeforbundne tjenester. Formålet med et IXP er at sammenkoble net, som er teknisk og organisatorisk adskilte. Udtrykket »autonomt system« bruges til at beskrive et teknisk selvstændigt net.
- (19) Medlemsstaterne bør være ansvarlige for at fastlægge, hvilke enheder der opfylder kriterierne i definitionen af operatør af væsentlige tjenester. For at sikre en ensartet tilgang bør definitionen af operatør af væsentlige tjenester anvendes konsekvent i alle medlemsstater. Til dette formål fastlægger direktivet bestemmelser om vurderingen af enheder, der er aktive i særlige sektorer og delsektorer, opstilling af en liste over væsentlige tjenester, overvejelse af en fælles liste over tværsektorielle forhold for at fastslå, hvorvidt en potentiel hændelse ville have en væsentlig forstyrrende virkning, en høringsproces med inddragelse af relevante medlemsstater i tilfælde af enheder, der leverer tjenester i mere end én medlemsstat, og støtte af samarbejdsgruppen i identifikationsprocessen. For at sikre, at eventuelle ændringer på markedet afspejles korrekt, bør listen over identificerede operatører løbende tages op til revision i medlemsstaterne og om nødvendigt ajourføres. Endelig bør medlemsstaterne give Kommissionen de fornødne oplysninger for at vurdere, i hvilket omfang denne fælles fremgangsmåde har givet mulighed for en konsekvent anvendelse af definitionen i medlemsstaterne.
- (20) I forbindelse med identificering af operatører af væsentlige tjenester bør medlemsstaterne vurdere, i det mindste for hver delsektor, der er omhandlet i dette direktiv, hvilke tjenester der skal anses for at være væsentlige for opretholdelsen af kritiske samfundsmæssige og økonomiske aktiviteter, og om de enheder, der er opført på listen over de sektorer og delsektorer, der er omhandlet i dette direktiv, og som leverer disse tjenester, opfylder kriterierne for identificering af operatører. Ved vur-

deringen af, om en enhed leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, er det tilstrækkeligt at undersøge, om denne enhed yder en tjeneste, der er opført på listen over væsentlige tjenester. Det bør desuden påvises, at leveringen af væsentlige tjenester afhænger af net- og informationssystemer. Endelig skal medlemsstaterne ved vurderingen af, om en hændelse vil have en væsentlig forstyrrende virkning på leveringen af tjenesten, tage hensyn til en række tværsektorielle forhold samt, hvis det er relevant, sektorspecifikke forhold.

- (21) Med henblik på at identificere operatører af væsentlige tjenester forstås ved etablering i en medlemsstat en effektiv og reel udøvelse af aktiviteter gennem stabile ordninger. De pågældende ordningers retlige form, hvad enten det er gennem en filial eller et datterselskab med status af juridisk person, har ikke afgørende betydning i denne forbindelse.
- (22) Det er muligt, at enheder, der opererer i de sektorer og delsektorer, der er omhandlet i dette direktiv, både leverer væsentlige og ikkevæsentlige tjenester. Inden for luftfartssektoren leverer lufthavne eksempelvis tjenester, der af en medlemsstat kan betragtes som værende væsentlige, f.eks. forvaltning af start- og landingsbaner, men også en række tjenester, der kan betragtes som ikkevæsentlige, f.eks. tilvejebringelse af butiksområder. Operatører af væsentlige tjenester bør kun være omfattet af de særlige sikkerhedskrav, når det gælder tjenester, der betragtes som værende væsentlige. Med henblik på identificering af operatører bør medlemsstaterne derfor opstille en liste over de tjenester, der betragtes som væsentlige.
- (23) Listen over tjenester bør indeholde alle tjenester på en given medlemsstats område, der opfylder kravene i dette direktiv. Medlemsstaterne bør kunne supplere den eksisterende liste ved at tilføje nye tjenester. Listen over tjenester bør tjene som referencepunkt for medlemsstaterne med henblik på identificering af operatører af væsentlige tjenester. Listens formål er at identificere de typer af væsentlige tjenester, der findes i en given sektor omhandlet i dette direktiv, så de kan holdes adskilt fra ikkevæsentlige aktiviteter, for hvilke en enhed, der er aktiv i en given sektor, kan være ansvarlig. Listen over tjenester, der fastlægges af hver medlemsstat, vil kunne tjene som et yderligere input i vurderingen af den lovgivningsmæssige praksis i hver medlemsstat, så der kan sikres en overordnet sammenhæng i identifikationsprocessen blandt medlemsstaterne.
- (24) Når en enhed leverer en væsentlig tjeneste i to eller flere medlemsstater, bør disse medlemsstater med henblik på identifikationsprocessen deltage i bilaterale eller multilaterale drøftelser med hinanden. Denne høringsproces skal hjælpe dem med at vurdere operatørens kritiske karakter med hensyn til grænseoverskridende konsekvenser, hvilket giver hver af de involverede medlemsstater mulighed for at fremlægge deres synspunkter om de risici, der er forbundet med de leverede tjenester. De berørte medlemsstater bør tage hensyn til hinandens synspunkter i denne proces og bør kunne anmode om samarbejdsgruppens bistand i denne henseende.

- 
- (25) Som følge af identifikationsprocessen bør medlemsstaterne vedtage nationale foranstaltninger til at afgøre, hvilke enheder der er underkastet forpligtelser vedrørende sikkerhed i net- og informationssystemer. Dette resultat kan opnås ved at udarbejde en liste over alle operatører af væsentlige tjenester eller vedtage nationale foranstaltninger, herunder objektive målbare kriterier, som f.eks. operatørens produktion eller antallet af brugere, hvilket gør det muligt at fastslå, hvilke enheder der er underlagt forpligtelser vedrørende sikkerhed i net- og informationssystemer. De nationale foranstaltninger, hvad enten de allerede eksisterer eller vedtages i forbindelse med dette direktiv, bør omfatte alle retlige foranstaltninger, administrative foranstaltninger og politikker, der gør det muligt at identificere operatører af væsentlige tjenester i medfør af dette direktiv.
- (26) For at give en indikation af, hvor væsentlige de identificerede operatører af væsentlige tjenester er i forhold til den pågældende sektor, bør medlemsstaterne tage hensyn til antallet og størrelsen af disse operatører, f.eks. med hensyn til markedsandel, eller den producerede eller transporterede kvantitet, uden at være forpligtet til at videregive oplysninger, som ville afsløre, hvilke operatører der er blevet identificeret.
- (27) For at afgøre, hvorvidt en hændelse ville have en væsentlig forstyrrende virkning for levering af en væsentlig tjeneste, bør medlemsstaterne tage hensyn til en række forskellige faktorer, som f.eks. det antal brugere, der er afhængige af denne tjeneste til private eller erhvervs-mæssige formål. Brugen af denne tjeneste kan ske direkte, indirekte eller ved formidling. Ved vurderingen af, hvilke konsekvenser en hændelse kunne have rent omfangs- og varighedsmæssigt på økonomiske og samfundsmæssige aktiviteter eller den offentlige sikkerhed, bør medlemsstaterne ligeledes undersøge, hvor lang tid der skønnes at ville gå, før diskontinuiteten ville begynde at have negative konsekvenser.
- (28) Med henblik på at fastslå, hvorvidt en hændelse ville have en væsentlig forstyrrende virkning på leveringen af en væsentlig tjeneste, bør medlemsstaterne i tillæg til tværsektorielle forhold også tage højde for sektorspecifikke forhold. Med hensyn til energileverandører kan sådanne forhold f.eks. omfatte omfanget eller andelen af elektricitet, der er produceret på nationalt plan; for olieleverandører mængden pr. dag; for lufttransport, herunder lufthavne og luftfartsselskaber, jernbanetransport og søhavne, den nationale andel af trafikmængden og antallet af passagerer eller fragtoperationer årligt; for banker eller finansielle markedsinfrastrukturer deres systemiske betydning baseret på de samlede aktiver eller de samlede aktiver i forhold til BNP; for sundhedssektoren antallet af patienter under tjenesteyderens pleje pr. år; for vandproduktion, -behandling og -forsyning mængden og antallet samt typerne af brugere, der forsynes, herunder for eksempel hospitaler, organisationer for offentlige tjenester eller enkeltpersoner, og om der findes alternative vandkilder til dækning af samme geografiske område.
- (29) Hver medlemsstat bør have en national strategi for sikkerheden i net- og informationssystemer, der fastlægger, hvilke strategiske mål og konkrete politiktiltag der skal gennemføres for at nå og bibeholde et højt sikkerhedsniveau i net- og informationssystemer.
- (30) I betragtning af forskellene mellem nationale forvaltningsstrukturer og med henblik på at sikre allerede eksisterende sektorforanstaltninger eller Unionens tilsyns- og kontrolorganer og undgå overlappinger bør medlemsstaterne kunne udpege mere end én national kompetent myndighed med ansvar for udførelsen af de opgaver, som er knyttet til sikkerheden i net- og informationssystemer hos operatører af væsentlige tjenester og udbydere af digitale tjenester i henhold til dette direktiv.
- (31) For at fremme grænseoverskridende samarbejde og kommunikation og for at sikre en effektiv gennemførelse af dette direktiv er det nødvendigt, at hver medlemsstat, uden at det berører sektorspeci-

fikke kontrolordninger, udpeger ét nationalt centralt kontaktpunkt med ansvar for at koordinere spørgsmål vedrørende sikkerheden i net- og informationssystemer samt grænseoverskridende samarbejde på EU-plan. Kompetente myndigheder og centrale kontaktpunkter bør have tilstrækkelige tekniske, finansielle og menneskelige ressourcer til at sikre, at de på en effektiv måde kan udføre de opgaver, som de pålægges, og dermed opfylde målene i dette direktiv. Da dette direktiv har til formål at forbedre det indre markeds funktion ved at skabe tryghed og tillid, er medlemsstaterne nødt til at kunne samarbejde effektivt med de økonomiske aktører og struktureres i overensstemmelse hermed.

- (32) Kompetente myndigheder eller enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), bør modtage underretninger om hændelser. De centrale kontaktpunkter bør ikke direkte modtage nogen underretninger om hændelser, medmindre de også handler som en kompetent myndighed eller som en CSIRT. En kompetent myndighed eller en CSIRT bør imidlertid kunne give det centrale kontaktpunkt til opgave at fremsende underretninger om hændelser til de centrale kontaktpunkter i andre berørte medlemsstater.
- (33) For at sikre en effektiv tilvejebringelse af oplysninger til medlemsstaten og Kommissionen bør den sammenfattende rapport forelægges af det centrale kontaktpunkt for samarbejdsgruppen, og den bør anonymiseres for at sikre, at underretningerne og identiteten af operatører af væsentlige tjenester og udbydere af digitale tjenester forbliver fortrolige, eftersom oplysninger om de underrettede enheders identitet ikke er påkrævet for udvekslingen af bedste praksis i samarbejdsgruppen. Den sammenfattende rapport bør indeholde oplysninger om antallet af modtagne underretninger og karakteren af de underrettede hændelser, f.eks. typerne af brud på sikkerheden, deres alvorlighed eller deres varighed.
- (34) Medlemsstaterne bør være udstyret med både tilstrækkelig teknisk og organisatorisk kapacitet, til at forebygge, detektere, reagere på og afhjælpe hændelser og risici i net- og informationssystemer. Alle medlemsstater bør derfor sikre sig, at de har velfungerende CSIRT'er, også kendt som IT-beredskabsenheder («CERT'er»), som opfylder de væsentlige krav for at sikre en effektiv og kompatibel kapacitet til at reagere på hændelser og risici og sikre et effektivt samarbejde på EU-plan. For at alle typer af operatører af væsentlige tjenester og udbydere af digitale tjenester kan få gavn af disse kapaciteter og dette samarbejde, bør medlemsstaterne sikre, at alle typer er omfattet af en udpeget CSIRT. I betragtning af betydningen af internationalt samarbejde om cybersikkerhed bør CSIRT'er kunne deltage i internationale samarbejdsnetværk i tillæg til de CSIRT-netværk, der er oprettet ved dette direktiv.
- (35) Da de fleste net- og informationssystemer er privatejede, er samarbejde mellem den offentlige og private sektor afgørende. Operatører af væsentlige tjenester og udbydere af digitale tjenester bør tilskyndes til at benytte deres egne uformelle samarbejdsmekanismer for at sikre sikkerheden i net- og informationssystemer. Samarbejdsgruppen bør, hvis det er relevant, kunne indbyde relevante interessenter til drøftelser. For effektivt at fremme udvekslingen af oplysninger og bedste praksis er det afgørende at sikre, at operatører af væsentlige tjenester og udbydere af digitale tjenester, som deltager i en sådan udveksling, ikke stilles dårligere som følge af deres samarbejde.
- (36) ENISA bør bistå medlemsstaterne og Kommissionen med ekspertise og rådgivning og ved at lette udveksling af bedste praksis. Især ved anvendelsen af dette direktiv bør Kommissionen, og medlemsstaterne bør kunne, rådføre sig med ENISA. Med sigte på opbygning af kapacitet og viden blandt medlemsstaterne bør samarbejdsgruppen også fungere som et redskab til udveksling af bedste praksis og drøftelse af medlemsstaternes kapaciteter og beredskab, og den bør på frivillig basis

bistå medlemmerne med evaluering af nationale strategier for sikkerheden i net- og informationssystemer, arbejde med kapacitetsopbygning og evaluering af øvelser vedrørende sikkerheden i net- og informationssystemer.

- (37) Medlemsstaterne bør, hvis det er relevant, kunne benytte eller tilpasse eksisterende organisationsstrukturer eller -strategier, når de anvender dette direktiv.
- (38) Samarbejdsgruppens og ENISA's respektive opgaver er indbyrdes afhængige og supplerer hinanden. Generelt bør ENISA bistå samarbejdsgruppen med udførelsen af dens opgaver i overensstemmelse med målet i Europa-Parlamentets og Rådets forordning (EU) nr. 526/2013<sup>7)</sup>, nemlig ved at bistå Unionens institutioner, organer, kontorer og agenturer og medlemsstaterne med at gennemføre de politikker, der er nødvendige for at opfylde de retlige og reguleringsmæssige krav vedrørende sikkerheden i net- og informationssystemer i henhold til eksisterende og fremtidige EU-retsakter. ENISA bør navnlig yde bistand på de områder, der svarer til dets egne opgaver, jf. forordning (EU) nr. 526/2013, nemlig at analysere sikkerhedsstrategier for net- og informationssystemer, støtte tilrettelæggelsen og gennemførelsen af EU-øvelser vedrørende sikkerheden i net- og informationssystemer og udveksle oplysninger og bedste praksis for bevidstgørelse og uddannelse. ENISA bør også deltage i udarbejdelsen af retningslinjer for sektorspecifikke kriterier for fastlæggelse af omfanget af en hændelses konsekvenser.
- (39) For at fremme forbedret sikkerhed i net- og informationssystemer bør samarbejdsgruppen, hvis det er relevant, samarbejde med relevante EU-institutioner, -organer, -kontorer og -agenturer med henblik på at udveksle knowhow og bedste praksis og yde rådgivning om sikkerhedsaspekter i net- og informationssystemer, der kan have konsekvenser for deres arbejde, samtidig med at den respekterer gældende ordninger for udveksling af fortrolige oplysninger. I samarbejdet med retshåndhavende myndigheder vedrørende sikkerhedsaspekter i net- og informationssystemer, der kan have konsekvenser for disse myndigheders arbejde, bør samarbejdsgruppen respektere eksisterende informationskanaler og etablerede net.
- (40) Oplysninger om hændelser er stadig mere værdifulde for den brede offentlighed og virksomheder, navnlig små og mellemstore virksomheder. I nogle tilfælde er der allerede adgang til disse oplysninger via websteder på nationalt plan på et bestemt lands sprog og med fokus på hændelser og begivenheder, der har en national dimension. Da virksomhederne i stigende grad opererer på tværs af grænserne, og borgerne benytter onlinetjenester, bør oplysninger om hændelser gives i sammenfattet form på EU-plan. CSIRT-netværkets sekretariat tilskyndes til at oprette et websted eller vedligeholde en særlig side på et eksisterende websted, hvor generelle oplysninger om større hændelser, som har fundet sted i hele Unionen, stilles til rådighed for den brede offentlighed med særlig fokus på virksomhedernes interesser og behov. CSIRT'er, der deltager i CSIRT-netværket, tilskyndes til på frivillig basis at levere de oplysninger, der skal offentliggøres på det nævnte websted, uden at der medtages fortrolige eller følsomme oplysninger.
- (41) Hvis oplysningerne betragtes som værende fortrolige i overensstemmelse med EU-regler og nationale regler om forretningshemmeligheder, bør denne fortrolighed sikres under udførelsen af aktiviteterne og opfyldelsen af målene i dette direktiv.
- (42) Øvelser, der simulerer hændesscenarier i realtid, er afgørende for testningen af medlemsstaternes beredskab og samarbejde vedrørende sikkerheden i net- og informationssystemer. Øvelsesforløbet Cyber Europe, som ENISA koordinerer med medlemsstaternes deltagelse, er et nyttigt redskab til testning og udarbejdelse af anbefalinger til, hvordan håndteringen af hændelser på EU-plan bør for-

bedres over tid. Eftersom medlemsstaterne ikke for øjeblikket er forpligtet til hverken at planlægge eller deltage i øvelser, bør oprettelsen af CSIRT-netværket i henhold til dette direktiv give dem mulighed for at deltage i øvelser på grundlag af præcis planlægning og strategiske valg. Den samarbejdsgruppe, der er nedsat i henhold til dette direktiv, bør drøfte de strategiske beslutninger vedrørende øvelser, navnlig, men ikke udelukkende, med hensyn til øvelsernes hyppighed og udformningen af scenarierne. ENISA bør i overensstemmelse med sit mandat støtte tilrettelæggelsen og gennemførelsen af EU-dækkende øvelser ved at bistå samarbejdsgruppen og CSIRT-netværket med ekspertise og rådgivning.

- (43) I betragtning af den globale karakter af sikkerhedsproblemer, der påvirker net- og informationssystemer, er der behov for et tættere internationalt samarbejde om at forbedre sikkerhedsstandarderne og informationsudvekslingen og for at fremme en fælles samlet tilgang til sikkerhedsspørgsmål.
- (44) Ansvar for at sikre sikkerheden i net- og informationssystemer ligger i vid udstrækning hos operatører af væsentlige tjenester og udbydere af digitale tjenester. En risikostyringskultur med risikovurdering og gennemførelse af sikkerhedsforanstaltninger, som står i forhold til risiciene, bør fremmes og udvikles gennem passende forskriftsmæssige krav og en frivillig indsats fra erhvervslivets side. Etablering af pålidelige lige vilkår er også afgørende for, at samarbejdsgruppen og CSIRT-netværket er velfungerende, så man sikrer et effektivt samarbejde fra alle medlemsstater.
- (45) Dette direktiv finder kun anvendelse på de offentlige myndigheder, der er identificeret som operatører af væsentlige tjenester. Det er derfor medlemsstaternes ansvar at sikre sikkerheden i net- og informationssystemer tilhørende offentlige myndigheder, som ikke henhører under dette direktivs anvendelsesområde.
- (46) Risikostyringsforanstaltninger omfatter foranstaltninger til at identificere alle risici for hændelser, forebygge, detektere og håndtere hændelser og begrænse deres konsekvenser. Sikkerheden i net- og informationssystemer omfatter lagrede, overførte og behandlede datas sikkerhed.
- (47) Kompetente myndigheder bør fortsat have mulighed for at vedtage nationale retningslinjer om de omstændigheder, hvorunder operatører af væsentlige tjenester har pligt til at underrette om hændelser.
- (48) Mange virksomheder i Unionen er afhængige af udbydere af digitale tjenester til levering af deres tjenester. Da nogle digitale tjenester kan være en vigtig ressource for deres brugere, herunder operatører af væsentlige tjenester, og brugerne af den grund måske ikke altid har nogen alternativer, bør dette direktiv også finde anvendelse på udbydere af denne type tjenester. Sikkerheden og kontinuiteten i samt pålideligheden af denne type digitale tjenester, der er omhandlet i dette direktiv, er for mange virksomheder afgørende for, at de fungerer godt. En afbrydelse af en sådan digital tjeneste kunne forhindre levering af andre tjenester, der er afhængige af den, og kunne dermed få konsekvenser for økonomiske og samfundsmæssige nøgleaktiviteter i Unionen. Sådanne digitale tjenester kan derfor have afgørende betydning for, at virksomheder, der er afhængige af dem, fungerer godt, og for, at disse virksomheder kan deltage i det indre marked og i grænseoverskridende handel i hele Unionen. De nævnte udbydere af digitale tjenester, der er omfattet af dette direktiv, er de udbydere, der anses for at tilbyde digitale tjenester, som mange virksomheder i Unionen i stigende grad er afhængige af.
- (49) Udbydere af digitale tjenester bør sikre et sikkerhedsniveau, der afspejler graden af den risiko, som de digitale tjenester, de leverer, udsættes for, i betragtning af den betydning, deres tjenester har for aktiviteter, der udføres af andre virksomheder i Unionen. I praksis vil graden af risiko for operatø-



rer af væsentlige tjenester, som ofte er af væsentlig betydning for opretholdelsen af vigtige økonomiske og samfundsmæssige aktiviteter, være højere end for udbydere af digitale tjenester. Derfor bør sikkerhedskravene for udbydere af digitale tjenester være mere moderate. Udbydere af digitale tjenester bør fortsat kunne træffe de foranstaltninger, som de mener er passende for at styre de risici, som sikkerheden i deres net- og informationssystemer udsættes for. Udbydere af digitale tjenester bør som følge af deres grænseoverskridende karakter omfattes af en mere harmoniseret tilgang på EU-plan. Gennemførelsesretsakter bør lette specificeringen og gennemførelsen af sådanne foranstaltninger.

- (50) Selv om hardwarefabrikanter og softwareudviklere hverken er operatører af væsentlige tjenester eller udbydere af digitale tjenester, forbedrer deres produkter sikkerheden i net- og informationssystemer. De spiller derfor en vigtig rolle for, at operatører af væsentlige tjenester og udbydere af digitale tjenester kan sikre deres net- og informationssystemer. Sådanne hardware- og softwareprodukter er allerede underlagt gældende regler om produktansvar.
- (51) Tekniske og organisatoriske foranstaltninger, der pålægges operatører af væsentlige tjenester og udbydere af digitale tjenester, bør ikke kræve, at et bestemt kommercielt informations- og kommunikationsteknologiproduct skal konstrueres, udvikles eller fremstilles på en bestemt måde.
- (52) Operatørerne af væsentlige tjenester og udbyderne af digitale tjenester bør sikre beskyttelsen af de net- og informationssystemer, de anvender. Det er hovedsageligt private net- og informationssystemer, hvor administrationen varetages af deres eget IT-personale, eller hvor sikkerhedsopgaverne er outsourcet. Sikkerhedskravene og underretningspligten bør gælde for de relevante operatører af væsentlige tjenester og udbydere af digitale tjenester, uanset om de selv står for vedligeholdelsen af deres net- og informationssystemer eller outsourcer denne opgave.
- (53) Med sigte på at undgå, at operatører af væsentlige tjenester og udbydere af digitale tjenester pålægges en uforholdsmæssig stor finansiel og administrativ byrde, bør kravene stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende net- og informationssystem, under hensyntagen til sådanne foranstaltningers aktuelle stade. For så vidt angår udbydere af digitale tjenester, bør disse krav ikke gælde for mikrovirksomheder og små virksomheder.
- (54) Når offentlige myndigheder i medlemsstaterne anvender tjenester, der tilbydes af udbydere af digitale tjenester, navnlig cloud computing-tjenester, vil de måske ønske at stille krav til udbyderne af disse tjenester om flere sikkerhedsforanstaltninger end dem, som udbydere af digitale tjenester normalt tilbyder i overensstemmelse med kravene i dette direktiv. De bør kunne gøre dette ved hjælp af kontraktlige forpligtelser.
- (55) Definitionerne af onlinemarkedsplads, onlinesøgemaskiner og cloud computing-tjenester i dette direktiv er specifikke for dette direktiv og berører ikke andre instrumenter.
- (56) Dette direktiv bør ikke forhindre medlemsstaterne i at vedtage nationale foranstaltninger, der forpligter offentligretlige organer til at sikre særlige sikkerhedskrav, når de indgår aftaler om cloud computing-tjenester. Sådanne nationale foranstaltninger bør finde anvendelse på den pågældende offentlige myndighed og ikke udbyderen af cloud computing-tjenester.
- (57) I betragtning af de grundlæggende forskelle mellem operatører af væsentlige tjenester, navnlig deres direkte forbindelse til fysisk infrastruktur, og udbydere af digitale tjenester, navnlig deres grænseoverskridende karakter, bør dette direktiv benytte en differentieret tilgang med hensyn til harmoniseringsniveauet i forbindelse med disse to grupper af enheder. For operatører af væsentlige tjene-

ster bør medlemsstaterne kunne identificere de relevante operatører og indføre strengere krav end dem, der er fastsat i dette direktiv. Medlemsstaterne bør ikke identificere udbydere af digitale tjenester, eftersom dette direktiv bør gælde for alle udbydere af digitale tjenester inden for dets anvendelsesområde. Desuden bør dette direktiv og de gennemførelsesretsakter, der vedtages i henhold hertil, sikre et højt harmoniseringsniveau for udbydere af digitale tjenester med hensyn til sikkerhedskrav og underretningspligt. Dette bør sætte udbyderne af digitale tjenester i stand til at blive behandlet på en ensartet måde i hele Unionen og på en måde, der står i rimeligt forhold til deres karakter og graden af den risiko, de kunne blive udsat for.

- (58) Dette direktiv bør ikke forhindre medlemsstaterne i at indføre sikkerhedskrav og underretningspligt for enheder, der ikke er udbydere af digitale tjenester inden for rammerne af dette direktiv, idet dette ikke berører medlemsstaternes forpligtelser i henhold til EU-retten.
- (59) De kompetente myndigheder bør tage behørigt hensyn til nødvendigheden af at bevare uformelle og pålidelige kanaler til informationsudveksling. Ved offentliggørelse af hændelser, der underrettes til de kompetente myndigheder, bør der foretages en nøje afvejning af offentlighedens interesse i at blive informeret om trusler i forhold til mulig imageskade og kommerciel skade for de operatører af væsentlige tjenester og udbydere af digitale tjenester, der underretter om hændelser. Ved gennemførelsen af underretningspligten bør de kompetente myndigheder og CSIRT'erne være særlig opmærksomme på behovet for at holde oplysninger om produkters sårbarhed strengt fortrolige, indtil der udsendes passende sikkerhedsopdateringer.
- (60) Udbydere af digitale tjenester bør underkastes et lempeligere og reaktivt efterfølgende tilsyn under hensyn til arten af deres tjenester og operationer. Den berørte kompetente myndighed bør derfor kun skride til handling, når den har fået dokumentation (f.eks. fra udbyderen af digitale tjenester selv, fra en anden kompetent myndighed, herunder en kompetent myndighed i en anden medlemsstat, eller fra brugeren af tjenesten) for, at en udbyder af digitale tjenester ikke overholder kravene i dette direktiv, navnlig efter at der er sket en hændelse. Den kompetente myndighed bør således ikke have en generel forpligtelse til at føre tilsyn med udbydere af digitale tjenester.
- (61) De kompetente myndigheder bør have de nødvendige midler til at udføre deres opgaver, herunder beføjelser til at indhente tilstrækkelige oplysninger til, at de kan vurdere sikkerhedsniveauet i net- og informationssystemer.
- (62) Hændelser kan være resultatet af kriminelle aktiviteter, og forebyggelse, efterforskning og retsforfølgelse heraf støttes ved koordinering og samarbejde mellem operatører af væsentlige tjenester, udbydere af digitale tjenester, kompetente myndigheder og retshåndhævende myndigheder. Hvis der er mistanke om, at en hændelse er forbundet med alvorlige kriminelle aktiviteter i henhold til EU-retten eller national ret, bør medlemsstaterne tilskynde operatører af væsentlige tjenester og udbydere af digitale tjenester til at underrette om hændelser af formodet alvorlig kriminel karakter til de relevante retshåndhævende myndigheder. Hvis det er relevant, er det ønskværdigt, at koordineringen mellem forskellige medlemsstaters kompetente myndigheder og retshåndhævende myndigheder lettes af det Europæiske Center til Bekæmpelse af IT-Kriminalitet (EC3) og ENISA.
- (63) Personoplysninger er i mange tilfælde kompromitteret som følge af hændelser. De kompetente myndigheder og databeskyttelsesmyndighederne bør i denne forbindelse samarbejde og udveksle oplysninger om alle relevante spørgsmål for at håndtere alle brud på persondatasikkerheden som følge af hændelser.

- (64) Jurisdiktion, for så vidt angår udbydere af digitale tjenester, bør tildeles den medlemsstat, hvor den pågældende udbyder af digitale tjenester har sit hjemsted i Unionen, hvilket i princippet svarer til det sted, hvor udbyderen har sit hovedkontor i Unionen. Ved hjemsted forstås en effektiv og reel udøvelse af aktivitet gennem stabile ordninger. De pågældende ordningers retlige form, hvad enten det er en filial eller et datterselskab med status af juridisk person, har ikke afgørende betydning i denne forbindelse. Dette kriterium bør ikke afhænge af, hvorvidt net- og informationssystemerne fysisk befinder sig på et givent sted; tilstedeværelsen og anvendelsen af sådanne systemer udgør ikke i sig selv et sådant hjemsted og er derfor ikke et kriterium for fastlæggelse af hjemstedet.
- (65) En udbyder af digitale tjenester, som ikke er etableret i Unionen, men tilbyder tjenester i Unionen, bør udpege en repræsentant. Med henblik på at afgøre, om en sådan udbyder af digitale tjenester tilbyder tjenester i Unionen, bør det fastslås, om det er åbenbart, at udbyderen af digitale tjenester påtænker at tilbyde tjenester til personer i en eller flere medlemsstater. Alene det forhold, at der i Unionen er adgang til udbyderen af digitale tjenester eller en mellemmands websted eller til en e-mailadresse og andre kontaktoplysninger eller at der anvendes et sprog, som almindeligvis anvendes i det tredjeland, hvor udbyderen af digitale tjenester er etableret, er utilstrækkeligt til at fastslå en sådan hensigt. Imidlertid kan faktorer såsom anvendelse af et sprog eller en valuta, der almindeligvis anvendes i en eller flere medlemsstater med mulighed for at bestille tjenester på det pågældende sprog, eller omtale af kunder eller brugere, der er i Unionen, gøre det åbenbart, at udbyderen af digitale tjenester påtænker at tilbyde tjenester i Unionen. Repræsentanten bør handle på vegne af udbyderen af digitale tjenester, og kompetente myndigheder eller CSIRT'er bør kunne kontakte repræsentanten. Repræsentanten bør udtrykkeligt udpeges ved et skriftligt mandat fra udbyderen af digitale tjenester til at handle på sidstnævntes vegne, for så vidt angår sidstnævntes forpligtelser i medfør af dette direktiv, herunder underretning om hændelser.
- (66) Standardisering af sikkerhedskrav er en markedsstyret proces. Medlemsstaterne bør for at sikre en konvergerende anvendelse af sikkerhedsstandarder tilskynde til overholdelse af eller overensstemmelse med specificerede standarder for at sikre et højt sikkerhedsniveau i net- og informationssystemer på EU-plan. ENISA bør bistå medlemsstaterne med rådgivning og retningslinjer. Med dette mål for øje kan det være nyttigt at udarbejde udkast til harmoniserede standarder, som bør udformes i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012<sup>8)</sup>.
- (67) Enheder, der falder uden for dette direktivs anvendelsesområde, kan opleve hændelser, der har væsentlige konsekvenser for de tjenester, de leverer. Hvis disse enheder anser det for at være i offentlighedens interesse at underrette om forekomsten af sådanne hændelser, bør de kunne gøre det på et frivilligt grundlag. Sådanne underretninger bør behandles af den kompetente myndighed eller CSIRT, når en sådan behandling ikke udgør en uforholdsmæssig stor eller unødvendig byrde for de berørte medlemsstater.
- (68) For at sikre ensartede betingelser for gennemførelsen af dette direktiv bør Kommissionen tillægges gennemførelsesbeføjelser til at fastlægge de proceduremæssige ordninger, der er nødvendige for samarbejdsgruppens funktion, og de sikkerhedskrav og den underretningspligt, der gælder for udbydere af digitale tjenester. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011<sup>9)</sup>. Når Kommissionen vedtager gennemførelsesretsakter vedrørende de proceduremæssige ordninger, der er nødvendige for samarbejdsgruppens funktion, bør den tage størst muligt hensyn til udtalelsen fra ENISA.

- (69) Når Kommissionen vedtager gennemførelsesretsakter om sikkerhedskravene for udbydere af digitale tjenester, bør den tage størst muligt hensyn til udtalelsen fra ENISA og den bør konsultere de interesserede interessenter. Endvidere tilskyndes Kommissionen til at tage hensyn til følgende eksempler: vedrørende systemers og faciliteters sikkerhed: fysisk og miljømæssig sikkerhed, forsyningssikkerhed, kontrol af adgang til net- og informationssystemer og integritet i forbindelse med net- og informationssystemer; vedrørende håndtering af hændelser: procedurer for håndtering af hændelser, kapacitet til detektering af hændelser, underretning om og meddelelse af hændelser; vedrørende styring af driftskontinuitet: strategi for tjenesters kontinuitet og beredskabsplaner, katastrofeberedskabskapaciteter; vedrørende monitorering, audit og testning: monitorerings- og logningspolitikker, øvelsesberedskabsplaner, testning af net- og informationssystemer, sikkerhedsvurdering og kontrol med overholdelse.
- (70) I forbindelse med gennemførelsen af dette direktiv bør Kommissionen i passende omfang varetage kontakten med relevante sektorudvalg og relevante organer på EU-plan inden for de områder, der er omfattet af dette direktiv.
- (71) Kommissionen bør regelmæssigt tage dette direktivs bestemmelser op til fornyet overvejelse efter høring af interesserede interessenter, navnlig med henblik på at afgøre, om der er behov for ændringer i lyset af skiftende samfundsmæssige, politiske eller teknologiske vilkår eller markedsvilkår.
- (72) Udveksling af oplysninger om risici og hændelser i samarbejdsgruppen og CSIRT-netværket og overholdelse af kravet om underretning om hændelser til de nationale kompetente myndigheder eller CSIRT'er kan kræve behandling af personoplysninger. En sådan behandling bør ske i overensstemmelse med Europa-Parlamentets og Rådets direktiv 95/46/EF<sup>10)</sup> og Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001<sup>11)</sup>. I forbindelse med anvendelsen af dette direktiv bør Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001<sup>12)</sup> finde anvendelse i relevant omfang.
- (73) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001 og afgav en udtalelse den 14. juni 2013<sup>13)</sup>.
- (74) Målene for dette direktiv, nemlig at opnå et højt, fælles sikkerhedsniveau i net- og informationssystemer i Unionen, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går dette direktiv ikke videre, end hvad der er nødvendigt for at nå disse mål.
- (75) Dette direktiv overholder de grundlæggende rettigheder og de principper, der anerkendes i Den Europæiske Unions charter om grundlæggende rettigheder, navnlig retten til respekt for privatlivet og kommunikation, beskyttelsen af personoplysninger, frihed til at oprette og drive egen virksomhed, ejendomsretten og retten til effektive retsmidler for en domstol og ret til at blive hørt. Direktivet bør gennemføres i overensstemmelse med disse rettigheder og principper —

<sup>3)</sup> Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) (EFT L 108 af 24.4.2002, s. 33).

<sup>4)</sup> Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

<sup>5)</sup> Rådets afgørelse 2013/488/EU af 23. september 2013 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer (EUT L 274 af 15.10.2013, s. 1).

<sup>6)</sup> EUT C 352 af 7.10.2014, s. 4.

- 7) Europa-Parlamentets og Rådets forordning (EU) nr. 526/2013 af 21. maj 2013 om Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) og om ophævelse af forordning (EF) nr. 460/2004 (EUT L 165 af 18.6.2013, s. 41).
- 8) Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).
- 9) Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).
- 10) Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995, s. 31).
- 11) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001, s. 1).
- 12) Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter (EFT L 145 af 31.5.2001, s. 43).
- 13) EUT C 32 af 4.2.2014, s. 19.

VEDTAGET DETTE DIREKTIV:

## KAPITEL I

### GENERELLE BESTEMMELSER

#### Artikel 1

#### Genstand og anvendelsesområde

1. Dette direktiv fastsætter foranstaltninger med henblik på at opnå et højt fælles sikkerhedsniveau for net- og informationssystemer i Unionen for at forbedre det indre markeds funktion.

2. Direktivet:

- a) fastsætter forpligtelser for alle medlemsstater til at vedtage en national strategi for sikkerhed i net- og informationssystemer
- b) nedsætter en samarbejdsgruppe med henblik på at støtte og lette strategisk samarbejde og udveksling af oplysninger mellem medlemsstaterne og at skabe tillid blandt dem
- c) opretter et netværk af enheder, der håndterer IT-sikkerhedshændelser (»CSIRT-netværk«), med henblik på at bidrage til skabelsen af tillid mellem medlemsstaterne og at fremme et hurtigt og effektivt operationelt samarbejde
- d) fastsætter sikkerhedskrav og underretningspligt for operatører af væsentlige tjenester og for udbydere af digitale tjenester
- e) fastsætter forpligtelser for medlemsstaterne til at udpege nationale kompetente myndigheder, centrale kontaktpunkter og CSIRT'er, som pålægges opgaver relateret til sikkerheden i net- og informationssystemer

3. De sikkerhedskrav og den underretningspligt, der er fastsat i dette direktiv, anvendes ikke for virksomheder, som er omfattet af kravene i artikel 13a og 13b i direktiv 2002/21/EF, eller for tillidstjenesteudbydere, som er omfattet af kravene i artikel 19 i forordning (EU) nr. 910/2014.

4. Dette direktiv berører ikke Rådets direktiv 2008/114/EF<sup>14)</sup> og Europa-Parlamentets og Rådets direktiv 2011/93/EU<sup>15)</sup> og 2013/40/EU<sup>16)</sup>.

5. Oplysninger, der er fortrolige i henhold til EU-regler og nationale regler, som f.eks. regler om forretningshemmeligheder, udveksles med forbehold af artikel 346 i TEUF kun med Kommissionen og andre relevante myndigheder, hvis en sådan udveksling er nødvendig for anvendelsen af dette direktiv. De udvekslede oplysninger begrænses til, hvad der er relevant og forholdsmæssigt under hensyn til formålet med udvekslingen. En sådan udveksling af oplysninger skal sikre de nævnte oplysningers fortrolighed og

beskytte sikkerheden og kommercielle interesser hos operatører af væsentlige tjenester og udbydere af digitale tjenester.

6. Dette direktiv berører ikke de tiltag, som iværksættes af medlemsstaterne med henblik på at sikre deres centrale statslige funktioner, navnlig for at værne om den nationale sikkerhed, herunder foranstaltninger til beskyttelse af oplysninger, hvis udbredelse efter medlemsstaternes opfattelse ville stride mod deres væsentlige sikkerhedsinteresser, og opretholde lov og orden, navnlig for at tillade efterforskning, afsløring og retsforfølgelse af strafbare handlinger.

7. Når en sektorspecifik EU-retsakt stiller krav om, at operatører af væsentlige tjenester og udbydere af digitale tjenester enten skal sikre sikkerheden i deres net- og informationssystemer eller underrette om hændelser, forudsat at sådanne krav har mindst samme virkning som forpligtelserne i dette direktiv, anvendes de pågældende bestemmelser i den nævnte sektorspecifikke EU-retsakt.

## *Artikel 2*

### **Behandling af personoplysninger**

1. Behandling af personoplysninger i henhold til nærværende direktiv udføres i overensstemmelse med direktiv 95/46/EF.

2. Behandling af personoplysninger i EU-institutioner og -organer i henhold til nærværende direktiv gennemføres i overensstemmelse med forordning (EF) nr. 45/2001.

## *Artikel 3*

### **Minimumsharmonisering**

Uden at dette berører artikel 16, stk. 10, og deres forpligtelser i henhold til EU-retten, kan medlemsstaterne vedtage eller bibeholde bestemmelser, som har til formål at nå et højere sikkerhedsniveau for net- og informationssystemer.

## *Artikel 4*

### **Definitioner**

I dette direktiv forstås ved:

**1) »net- og informationssystem«:**

- a) et elektronisk kommunikationsnet som omhandlet i artikel 2, litra a), i direktiv 2002/21/EF
- c) 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

**2) »sikkerhed i net- og informationssystemer«:** 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

**3) »national strategi for sikkerheden i net- og informationssystemer«:** en ramme for strategiske mål og prioriteter for sikkerheden i net- og informationssystemer på nationalt plan

**4) »operatør af væsentlige tjenester«:** en offentlig eller privat enhed af en type som omhandlet i bilag II, der opfylder kriterierne i artikel 5, stk. 2

**5) »digital tjeneste«:** en tjeneste som omhandlet i artikel 1, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535<sup>17</sup>), som er af en type, der er opført i bilag III

**6) »udbyder af digitale tjenester«:** enhver juridisk person, som udbyder en digital tjeneste

**7) »hændelse«:** enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer

**8) »håndtering af hændelser«:** alle procedurer til støtte for detektering, analyse og begrænsning af en hændelse samt reaktionen derpå

**9) »risiko«:** enhver rimeligt identificerbar omstændighed eller begivenhed, der har en potentiel negativ indvirkning på sikkerheden i net- og informationssystemer

**10) »repræsentant«:** enhver fysisk eller juridisk person, der er etableret i Unionen, og som udtrykkeligt er udpeget til at handle på vegne af en udbyder af digitale tjenester, som ikke er etableret i Unionen, og som en national kompetent myndighed eller en CSIRT kan henvende sig til i stedet for udbyderen af digitale tjenester, for så vidt angår de forpligtelser, der påhviler den nævnte udbyder af digitale tjenester i medfør af dette direktiv

**11) »standard«:** en standard som omhandlet i artikel 2, nr. 1), i forordning (EU) nr. 1025/2012

**12) »specifikation«:** en teknisk specifikation som omhandlet i artikel 2, nr. 4), i forordning (EU) nr. 1025/2012

**13) »internetudvekslingspunkt (IXP)«:** en netfacilitet, som muliggør sammenkobling af mere end to uafhængige autonome systemer, hovedsageligt med henblik på at lette udvekslingen af internettrafik; et IXP leverer kun sammenkobling til autonome systemer; et IXP forudsætter 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

**14) »domænenavnesystem (DNS)«:** et hierarkisk opbygget navnesystem i et net, som behandler forespørgsler vedrørende domænenavne

**15) »DNS-tjenesteudbyder«:** en enhed, som leverer DNS-tjenester på internettet.

**16) »topdomænenavneadministrator«:** en enhed, som administrerer og driver registreringen af internetdomænenavne under et særligt topdomæne (TLD)

**17) »onlinemarkedsplads«:** en digital tjeneste, som giver forbrugere og/eller erhvervsdrivende som defineret i henholdsvis artikel 4, stk. 1, litra a) og b), i Europa-Parlamentets og Rådets direktiv 2013/11/EU<sup>18)</sup> mulighed for at indgå aftaler om køb eller tjenester online med erhvervsdrivende enten på onlinemarkedspladsens websted eller på et websted tilhørende en erhvervsdrivende, som anvender computing-tjenester, der udbydes af onlinemarkedspladsen

**18) »onlinesøgemaskine«:** en digital tjeneste, som giver brugerne mulighed for at foretage søgninger på principielt alle websteder eller websteder på et bestemt sprog på grundlag af en forespørgsel om et hvilket som helst emne ved hjælp af et søgeord, en sætning eller andet input, og som fremviser links, hvor der kan findes oplysninger om det ønskede indhold

**19) »cloud computing-tjeneste«:** en digital tjeneste, som giver adgang til en skalerbar og elastisk pulje af delbare IT-ressourcer

## *Artikel 5*

### **Identificering af operatører af væsentlige tjenester**

1. Senest den 9. november 2018 identificerer medlemsstaterne for hver sektor og delsektor, som er omhandlet i bilag II, de operatører af væsentlige tjenester, der er etableret på deres område.

2. De i artikel 4, nr. 4), omhandlede kriterier for identificering af operatører af væsentlige tjenester er følgende:

- a) en enhed leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/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.

3. Med henblik på stk. 1 udarbejder hver medlemsstat en liste over de i stk. 2, litra a), omhandlede tjenester.

4. Med henblik på stk. 1 hører disse medlemsstater hinanden, hvis en enhed leverer en tjeneste, der er omhandlet i stk. 2, litra a), i to eller flere medlemsstater. Denne høring skal finde sted, inden der træffes afgørelse om identificering.

5. Medlemsstaterne tager regelmæssigt og mindst hvert andet år efter den 9. maj 2018 listen over identificerede operatører af væsentlige tjenester op til revision og ajourfører den, hvis det er relevant.

6. Samarbejdsgruppens rolle skal i overensstemmelse med de i artikel 11 omhandlede opgaver være at støtte medlemsstaterne i at anvende en ensartet tilgang, når operatører af væsentlige tjenester identificeres.

7. Med henblik på den i artikel 23 omhandlede revision og senest den 9. november 2018 og herefter hvert andet år forelægger medlemsstaterne Kommissionen de oplysninger, som er nødvendige for, at Kommissionen kan vurdere gennemførelsen af dette direktiv, navnlig ensartetheden i medlemsstaternes fremgangsmåder ved identificeringen af operatører af væsentlige tjenester. Disse oplysninger skal som minimum omfatte:

- a) nationale foranstaltninger, som gør det muligt at identificere operatører af væsentlige tjenester
- b) den i stk. 3 omhandlede liste over tjenester
- c) det antal af operatører af væsentlige tjenester, som er identificeret for hver sektor, der er omhandlet i bilag II, og en angivelse af deres betydning i forhold til den pågældende sektor
- d) tærskler, hvis sådanne findes, til fastlæggelse af det relevante forsyningsniveau ved henvisning til antallet af brugere, der er afhængige af denne tjeneste, jf. artikel 6, stk. 1, litra a), eller til vigtigheden af den pågældende operatør af væsentlige tjenester, jf. artikel 6, stk. 1, litra f).

For at bidrage til at levere sammenlignelige oplysninger kan Kommissionen under størst mulig hensyntagen til udtalelsen fra ENISA vedtage passende tekniske retningslinjer for kriterier for de oplysninger, som er omhandlet i dette stykke.

### *Artikel 6*

#### **Væsentlig forstyrrende virkning**

1. Ved fastlæggelsen af betydningen af en forstyrrende virkning, jf. artikel 5, stk. 2, litra c), tager medlemsstaterne som minimum hensyn til følgende tværsektorielle forhold:

- a) antal af brugere, der er afhængige af de tjenester, som udbydes af den pågældende enhed
- b) afhængighed i andre sektorer som omhandlet i bilag II af den tjeneste, der leveres af den nævnte enhed
- c) de konsekvenser, som hændelser kan have med hensyn til omfang og varighed på økonomiske og samfundsmæssige aktiviteter eller den offentlige sikkerhed
- d) den nævnte enheds markedsandel
- e) den geografiske udbredelse med hensyn til det område, som kunne berøres af en hændelse
- f) enhedens betydning med henblik på at opretholde et tilstrækkeligt tjenesteniveau under hensyntagen til tilgængelige alternative måder til levering af denne tjeneste.

2. Med henblik på at fastslå, hvorvidt en hændelse vil have en væsentlig forstyrrende virkning, tager medlemsstaterne endvidere, hvis det er relevant, hensyn til sektorspecifikke forhold.

## **KAPITEL II**

### **NATIONALE RAMMER FOR SIKKERHEDEN I NET- OG INFORMATIONSSYSTEMER**

#### *Artikel 7*

#### **National strategi for sikkerheden i net- og informationssystemer**



1. Hver medlemsstat vedtager en national strategi for sikkerheden i net- og informationssystemer, som fastlægger de strategiske mål og passende politiske og lovgivningsmæssige foranstaltninger med henblik på at nå og opretholde et højt sikkerhedsniveau i net- og informationssystemer, og som mindst omfatter de i bilag II omhandlede sektorer og de i bilag III omhandlede tjenester. Den nationale strategi for sikkerheden i net- og informationssystemer skal navnlig behandle følgende emner:

- a) målene og de prioriterede områder i den nationale strategi for sikkerhed i net- og informationssystemer
- b) en styringsmæssig ramme for at nå målene og de prioriterede områder i den nationale strategi for sikkerhed i net- og informationssystemer, herunder de statslige organers og andre relevante aktørers roller og ansvar
- c) fastlæggelse af foranstaltninger vedrørende beredskab, reaktion og genopretning, herunder samarbejde mellem den offentlige og den private sektor
- d) en angivelse af teoretiske og praktiske uddannelsesprogrammer og oplysningsprogrammer i forbindelse med den nationale strategi for sikkerhed i net- og informationssystemer
- e) en angivelse af forsknings- og udviklingsplaner relateret til den nationale strategi for sikkerhed i net- og informationssystemer
- f) en risikovurderingsplan til brug ved identifikation af risici
- g) en liste over de forskellige aktører, der er involveret i gennemførelse af den nationale strategi for sikkerhed i net- og informationssystemer.

2. Medlemsstaterne kan anmode ENISA om bistand til at udvikle nationale strategier for sikkerhed i net- og informationssystemer.

3. Medlemsstaterne meddeler deres nationale strategier for sikkerhed i net- og informationssystemer til Kommissionen senest tre måneder efter vedtagelsen heraf. Medlemsstaterne kan i forbindelse hermed udelukke elementer i strategien, der vedrører national sikkerhed.

## *Artikel 8*

### **Nationale kompetente myndigheder og centralt kontaktpunkt**

1. Hver medlemsstat udpeger en eller flere nationale kompetente myndigheder for sikkerheden i net- og informationssystemer («kompetent myndighed»), som mindst omfatter de i bilag II omhandlede sektorer og de i bilag III omhandlede tjenester. Medlemsstaterne kan tildele en eller flere eksisterende myndigheder denne rolle.

2. De kompetente myndigheder fører tilsyn med anvendelsen af dette direktiv på nationalt plan.

3. Hver medlemsstat udpeger et nationalt centralt kontaktpunkt for sikkerheden i net- og informationssystemer («centralt kontaktpunkt»). Medlemsstaterne kan tildele en eksisterende myndighed denne rolle. Hvis en medlemsstat kun udpeger én kompetent myndighed, fungerer denne kompetente myndighed ligeledes som det centrale kontaktpunkt.

4. Det centrale kontaktpunkt udgør et forbindelsesled til at sikre grænseoverskridende samarbejde mellem medlemsstaternes myndigheder og de relevante myndigheder i andre medlemsstater samt den samarbejdsgruppe, der er omhandlet i artikel 11, og det i artikel 12 omhandlede CSIRT-netværk.

5. Medlemsstaterne sikrer, at de kompetente myndigheder og de centrale kontaktpunkter har tilstrækkelige ressourcer til på en effektiv måde at udføre de opgaver, som de pålægges, og dermed opfylde målene i dette direktiv. Medlemsstaterne sikrer et effektivt og sikkert samarbejde mellem de udpegede repræsentanter i samarbejdsgruppen.

6. De kompetente myndigheder og det centrale kontaktpunkt konsulterer og samarbejder, hvor det er passende og i henhold til national ret, med de relevante nationale retshåndhavende myndigheder og de nationale databeskyttelsesmyndigheder.

7. Hver medlemsstat underretter straks Kommissionen om udpegelsen af den kompetente myndighed og det centrale kontaktpunkt, deres opgaver og enhver senere ændring heraf. Hver medlemsstat offentliggør sin udpegelse af den kompetente myndighed og det centrale kontaktpunkt. Kommissionen offentliggør listen over udpegede centrale kontaktpunkter.

#### *Artikel 9*

##### **Enheder, der håndterer IT-sikkerhedshændelser (»CSIRT'er«)**

1. Hver medlemsstat udpeger en eller flere CSIRT'er, der skal opfylde kravene i bilag I, punkt 1, og som mindst omfatter de i bilag II omhandlede sektorer og de i bilag III omhandlede tjenester, og som er ansvarlige for at håndtere hændelser og risici i overensstemmelse med en nøje fastlagt proces. En CSIRT kan oprettes som en del af en kompetent myndighed.

2. Medlemsstaterne sikrer, at CSIRT'erne har tilstrækkelige ressourcer til effektivt at udføre deres opgaver som fastlagt i bilag I, punkt 2.

Medlemsstaterne sikrer et effektivt og sikkert samarbejde mellem deres CSIRT'er i det CSIRT-netværk, der er omhandlet i artikel 12.

3. Medlemsstaterne sikrer, at deres CSIRT'er har adgang til en passende, sikker og robust kommunikations- og informationsinfrastruktur på nationalt plan.

4. Medlemsstaterne oplyser Kommissionen om deres CSIRT'ers kompetenceområde og de vigtigste elementer i procedurerne for håndtering af hændelser.

5. Medlemsstaterne kan anmode ENISA om bistand til at udvikle nationale CSIRT'er.

#### *Artikel 10*

##### **Samarbejde på nationalt plan**

1. Hvis den samme medlemsstats kompetente myndighed, centrale kontaktpunkt og CSIRT er adskilte enheder, samarbejder de med hensyn til opfyldelsen af de forpligtelser, der er fastlagt i dette direktiv.

2. Medlemsstaterne sikrer, at enten de kompetente myndigheder eller CSIRT'erne modtager underretninger om hændelser, som fremsendes i henhold til dette direktiv. Hvis en medlemsstat beslutter, at CSIRT'er ikke skal modtage underretninger, skal CSIRT'erne, i det omfang det er nødvendigt, for at de kan udføre deres opgaver, have adgang til oplysninger om hændelser, der er underrettet af operatører af væsentlige tjenester i henhold til artikel 14, stk. 3 og 5, eller af udbydere af digitale tjenester i henhold til artikel 16, stk. 3 og 6.

3. Medlemsstaterne sikrer, at de kompetente myndigheder eller CSIRT'erne oplyser de centrale kontaktpunkter om underretninger om hændelser fremsendt i henhold til dette direktiv.

Senest den 9. august 2018 og derefter en gang om året forelægger det centrale kontaktpunkt samarbejdsgruppen en sammenfattende rapport om de underretninger, som det har modtaget, herunder antallet af underretninger og arten af de underrettede hændelser, samt de tiltag, der er iværksat i overensstemmelse med artikel 14, stk. 3 og 5, og artikel 16, stk. 3 og 5.

### **KAPITEL III**

#### **SAMARBEJDE**

#### *Artikel 11*

##### **Samarbejdsgruppe**

1. For at støtte og lette strategisk samarbejde og udvekslingen af oplysninger mellem medlemsstaterne samt for at skabe tillid samt med henblik på at opnå et højt fælles sikkerhedsniveau i net- og informationssystemer i Unionen oprettes der herved en samarbejdsgruppe.

Samarbejdsgruppen udfører sine opgaver på grundlag af toårige arbejdsprogrammer som omhandlet i stk. 3, andet afsnit.

2. Samarbejdsgruppen består af repræsentanter fra medlemsstaterne, Kommissionen og ENISA.

Samarbejdsgruppen kan, hvis det er relevant, indbyde repræsentanter fra de relevante interessenter til at deltage i arbejdet.

Sekretariatsopgaverne varetages af Kommissionen.

3. Samarbejdsgruppen har følgende opgaver:

- a) at give strategisk vejledning om aktiviteterne i det CSIRT-netværk, som oprettes i medfør af artikel 12
- b) at udveksle bedste praksis for udveksling af oplysninger vedrørende underretning om hændelser, jf. artikel 14, stk. 3 og 5, og artikel 16, stk. 3 og 6
- c) at udveksle bedste praksis mellem medlemsstaterne og i samarbejde med ENISA bistå medlemsstaterne med kapacitetsopbygning for at sikre sikkerheden i net- og informationssystemer
- d) at drøfte medlemsstaternes kapaciteter og beredskab og på frivillig basis evaluere nationale strategier for sikkerheden i net- og informationssystemer og CSIRT'ers effektivitet samt identificere bedste praksis
- e) at udveksle oplysninger og bedste praksis for oplysning og uddannelse
- f) at udveksle oplysninger og bedste praksis for forskning og udvikling i forbindelse med sikkerheden i net- og informationssystemer
- g) hvis det er relevant, at udveksle erfaringer om forhold vedrørende sikkerheden i net- og informationssystemer med Unionens relevante institutioner, organer, kontorer og agenturer
- h) at drøfte de i artikel 19 omhandlede standarder og specifikationer med repræsentanter fra de relevante europæiske standardiseringsorganisationer
- i) at indsamle oplysninger om bedste praksis i forbindelse med risici og hændelser
- j) årligt at gennemgå de sammenfattende rapporter som omhandlet i artikel 10, stk. 3, andet afsnit
- k) at drøfte det arbejde, som er udført med hensyn til øvelser vedrørende sikkerheden i net- og informationssystemer, teoretiske uddannelsesprogrammer og praktisk uddannelse, herunder det arbejde, som er udført af ENISA
- l) med ENISA's bistand at udveksle bedste praksis med hensyn til medlemsstaternes identificering af operatører af væsentlige tjenester, herunder i forbindelse med en grænseoverskridende afhængighed vedrørende risici og hændelser
- m) at drøfte metoder til rapportering af underretning om hændelser som omhandlet i artikel 14 og 16.

Senest den 9. februar 2018 og derefter hvert andet år udarbejder samarbejdsgruppen et arbejdsprogram vedrørende tiltag, der skal iværksættes for at gennemføre dens mål og opgaver, og som skal være i overensstemmelse med målene i dette direktiv.

4. Med henblik på den i artikel 23 omhandlede revision og senest den 9. august 2018 og derefter hver 18. måned udarbejder samarbejdsgruppen en rapport om de erfaringer, der er gjort med det strategiske samarbejde i medfør af denne artikel.

5. Kommissionen vedtager gennemførelsesretsakter, der fastsætter proceduremæssige ordninger, som er nødvendige for samarbejdsgruppens funktion. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 22, stk. 2.

Med henblik på første afsnit forelægger Kommissionen det første udkast til gennemførelsesretsakt for det i artikel 22, stk. 1, omhandlede udvalg senest den 9. februar 2017.

## *Artikel 12*

### **CSIRT-netværket**

1. Med henblik på at bidrage til skabelsen af tillid mellem medlemsstaterne og at fremme et hurtigt og effektivt operationelt samarbejde oprettes der herved et netværk af nationale CSIRT'er.

2. CSIRT-netværket består af repræsentanter fra medlemsstaternes CSIRT'er og CERT-EU. Kommissionen deltager i CSIRT-netværket som observatør. ENISA varetager sekretariatsopgaverne og støtter aktivt samarbejdet mellem CSIRT'erne.

3. CSIRT-netværket har følgende opgaver:

- a) at udveksle oplysninger om CSIRT'ers tjenester, aktiviteter og samarbejdsmuligheder
- b) på anmodning af en CSIRT-repræsentant fra en medlemsstat, som potentielt er berørt af en hændelse, at udveksle og drøfte oplysninger, der ikke er kommercielt følsomme, vedrørende denne hændelse og dermed forbundne risici; en medlemsstats CSIRT kan dog nægte at bidrage til denne drøftelse, hvis der er risiko for skade på efterforskningen af hændelsen
- c) at udveksle ikkefortrolige oplysninger om de enkelte hændelser og stille til dem rådighed på frivillig basis
- d) på anmodning af en repræsentant for en medlemsstats CSIRT at drøfte og, når det er muligt, identificere en samordnet reaktion på en hændelse, som er identificeret inden for den samme medlemsstats jurisdiktion
- e) at yde medlemsstater støtte i at håndtere grænseoverskridende hændelser med udgangspunkt i frivillig gensidig bistand
- f) at drøfte, undersøge og identificere yderligere former for operationelt samarbejde, herunder i forhold til:
  - i) kategorier af risici og hændelser
  - ii) tidlige varslinger
  - iii) gensidig bistand
  - iv) principper og retningslinjer for koordination, når medlemsstaterne reagerer på grænseoverskridende risici og hændelser
- g) at oplyse samarbejdsgruppen om sine aktiviteter og om yderligere former for operationelt samarbejde som drøftet i henhold til litra f) og anmode om vejledning i forbindelse hermed
- h) at drøfte erfaringer fra øvelser vedrørende sikkerheden i net- og informationssystemer, herunder fra øvelser, der afholdes af ENISA
- i) på anmodning af en given CSIRT at drøfte denne CSIRT's kapaciteter og beredskab
- j) at udstede retningslinjer for at lette konvergensen mellem operationel praksis med hensyn til anvendelsen af bestemmelserne i denne artikel vedrørende operationelt samarbejde.

4. Med henblik på den i artikel 23 omhandlede revision og senest den 9. august 2018 og derefter hver 18. måned udarbejder CSIRT-netværket en rapport om de erfaringer, der er gjort med det operationelle samarbejde, herunder konklusioner og anbefalinger, i medfør af denne artikel. Rapporten forelægges ligeledes for samarbejdsgruppen.

5. CSIRT-netværket fastlægger sin egen forretningsorden.

## *Artikel 13*

### **Internationalt samarbejde**

Unionen kan i overensstemmelse med artikel 218 i TEUF indgå internationale aftaler med tredjelande eller internationale organisationer, som giver disse mulighed for og tilrettelægger deres deltagelse i nogle af samarbejdsgruppens aktiviteter. En sådan aftale skal tage hensyn til behovet for at sikre tilstrækkelig beskyttelse af oplysninger.

## KAPITEL IV

### SIKKERHED I NET- OG INFORMATIONSSYSTEMER FOR OPERATØRER AF VÆSENTLIGE TJENESTER

#### *Artikel 14*

##### **Sikkerhedskrav og underretning om hændelser**

1. Medlemsstaterne sikrer, at operatører af væsentlige tjenester træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som de anvender til deres aktiviteter. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen.

2. Medlemsstaterne sikrer, at operatører af væsentlige tjenester træffer passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer, som anvendes til levering af sådanne væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester.

3. Medlemsstaterne sikrer, at operatører af væsentlige tjenester hurtigst muligt foretager en underretning til den kompetente myndighed eller CSIRT af hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Underretningerne skal indeholde oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. Underretning gør ikke den underrettede part til genstand for et øget ansvar.

4. Med henblik på at fastlægge omfanget af en hændelses konsekvenser tages navnlig følgende kriterier i betragtning:

- a) antallet af brugere, der berøres af afbrydelsen af den væsentlige tjeneste
- b) hændelsens varighed
- c) den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.

5. På grundlag af oplysningerne i den underretning, der er givet af operatøren af væsentlige tjenester, oplyser den kompetente myndighed eller CSIRT den eller de øvrige berørte medlemsstater herom, hvis hændelsen har væsentlige konsekvenser for kontinuiteten i de væsentlige tjenester i denne medlemsstat. I den forbindelse sikrer den kompetente myndighed eller CSIRT i overensstemmelse med EU-retten eller national lovgivning, der er i overensstemmelse med EU-retten, sikkerheden og de kommercielle interesser for operatøren af væsentlige tjenester samt fortrolig behandling af de oplysninger, der er givet i dennes underretning.

Hvis omstændighederne tillader det, leverer den kompetente myndighed eller CSIRT relevante oplysninger til den underrettede operatør af væsentlige tjenester vedrørende opfølgningen af dennes underretning, som f.eks. oplysninger, der kan støtte en effektiv håndtering af hændelsen.

På den kompetente myndigheds eller CSIRT's anmodning videresender de centrale kontaktpunkter de underretninger, der er omhandlet i første afsnit, til centrale kontaktpunkter i andre berørte medlemsstater.

6. Efter høring af den underrettede operatør af væsentlige tjenester kan den kompetente myndighed eller CSIRT'en oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

7. Kompetente myndigheder, der handler sammen inden for samarbejdsgruppen, kan udarbejde og vedtage retningslinjer om de omstændigheder, hvorunder operatører af væsentlige tjenester har pligt til at underrette om hændelser, herunder om kriterier for fastlæggelse af omfanget af en hændelses konsekvenser som omhandlet i stk. 4.

#### *Artikel 15*

## **Gennemførelse og håndhævelse**

1. Medlemsstaterne sikrer, at de kompetente myndigheder har de nødvendige beføjelser og midler til at vurdere, hvorvidt operatører af væsentlige tjenester opfylder deres forpligtelser i medfør af artikel 14 og virkningerne heraf på net- og informationssystemers sikkerhed.

2. Medlemsstaterne sikrer, at de kompetente myndigheder har beføjelser og midler til at pålægge operatører af væsentlige tjenester at levere:

- a) de oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker
- b) dokumentation for den faktiske gennemførelse af sikkerhedspolitikker, som f.eks. resultaterne af en sikkerhedsaudit udført af den kompetente myndighed eller en kvalificeret auditør og i sidstnævnte tilfælde stille resultaterne heraf, herunder den tilgrundliggende dokumentation, til rådighed for den kompetente myndighed.

Når der anmodes om sådanne oplysninger eller sådan dokumentation, angiver de kompetente myndigheder formålet med anmodningen og anfører, hvilke oplysninger der kræves.

3. Efter vurderingen af oplysninger eller resultaterne af sikkerhedsaudit, jf. stk. 2, kan den kompetente myndighed udstede påbud til operatører af væsentlige tjenester for at afhjælpe de påviste mangler.

4. Den kompetente myndighed indgår i et tæt samarbejde med databeskyttelsesmyndigheder, når de håndterer hændelser, som medfører brud på persondatasikkerheden.

## **KAPITEL V**

### **SIKKERHED I NET- OG INFORMATIONSSYSTEMER FOR UDBYDERE AF DIGITALE TJENESTER**

#### *Artikel 16*

#### **Sikkerhedskrav og underretning om hændelser**

1. Medlemsstaterne sikrer, at udbydere af digitale tjenester identificerer og træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene i forhold til sikkerheden i net- og informationssystemer, som de anvender i forbindelse med tjenester, der er omhandlet i bilag III, i Unionen. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen, under hensyntagen til følgende elementer:

- a) systemers og faciliteters sikkerhed
- b) håndtering af hændelser
- c) styring af driftskontinuitet
- d) monitorering, audit og testning
- e) overholdelse af internationale standarder.

2. Medlemsstaterne sikrer, at udbydere af digitale tjenester træffer foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i deres net- og informationssystemer, for så vidt angår de tjenester, der er omhandlet i bilag III, og som udbydes i Unionen, for at sikre kontinuiteten i disse tjenester.

3. Medlemsstaterne sikrer, at udbydere af digitale tjenester hurtigst muligt foretager en underretning til den kompetente myndighed eller CSIRT af enhver hændelse, der har betydelige konsekvenser for leveringen af en tjeneste som omhandlet i bilag III, som de udbyder i Unionen. Underretninger skal indeholde oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT at fastslå betydningen af eventuelle grænseoverskridende konsekvenser. Underretningen gør ikke den underrettende part genstand for et øget ansvar.

4. Med henblik på at fastlægge, om en hændelses konsekvenser er betydelige, tages navnlig følgende kriterier i betragtning:

- a) antallet af brugere, der berøres af hændelsen, navnlig brugere, som er afhængige af tjenesten med henblik på levering af deres egne tjenester
- b) hændelsens varighed
- c) den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen
- d) omfanget af afbrydelsen af tjenestens funktion
- e) omfanget af konsekvenserne for økonomiske og samfundsmæssige aktiviteter.

Forpligtelsen til at underrette om en hændelse finder kun anvendelse, hvis udbyderen af digitale tjenester har adgang til de oplysninger, der er nødvendige for at vurdere en hændelses konsekvenser i henhold til de i første afsnit omhandlede kriterier.

5. Når en operatør af væsentlige tjenester er afhængig af en tredjepartsudbyder af digitale tjenester vedrørende leveringen af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og økonomiske aktiviteter, underretter operatøren af væsentlige tjenester om alle væsentlige konsekvenser for de væsentlige tjenesters kontinuitet som følge af en hændelse, der berører den pågældende udbyder.

6. Hvis det er relevant, og navnlig hvis den hændelse, der er omhandlet i stk. 3, berører to eller flere medlemsstater, informerer den kompetente myndighed eller CSIRT de øvrige berørte medlemsstater. De kompetente myndigheder, CSIRT'erne og de centrale kontaktpunkter sikrer i den forbindelse i overensstemmelse med EU-retten eller national lovgivning, der er i overensstemmelse med EU-retten, den digitale tjenesteudbyders sikkerhed og kommercielle interesser samt fortrolig behandling af de givne oplysninger.

7. Efter høring af udbyderen af de digitale tjenester kan den kompetente myndighed eller CSIRT og, hvis det er relevant, myndighederne eller CSIRT'erne i andre berørte medlemsstater oplyse offentligheden om konkrete hændelser eller kræve, at udbyderen af digitale tjenester gør det, 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.

8. Kommissionen vedtager gennemførelsesretsakter for at fastsætte en yderligere specifikation af de elementer, der er omhandlet i nærværende artikels stk. 1, og de kriterier, der er opført i stk. 4. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 22, stk. 2, senest den 9. august 2017.

9. Kommissionen kan vedtage gennemførelsesretsakter, der fastsætter formater og procedurer for underretningspligten. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 22, stk. 2.

10. Medlemsstaterne må ikke indføre yderligere sikkerhedskrav eller underretningspligt for udbydere af digitale tjenester, jf. dog artikel 1, stk. 6.

11. Kapitel V finder ikke anvendelse på mikrovirksomheder og små virksomheder som defineret i Kommissionens henstilling 2003/361/EF<sup>19)</sup>.

## *Artikel 17*

### **Gennemførelse og håndhævelse**

1. Medlemsstaterne sikrer, at de kompetente myndigheder om nødvendigt griber ind ved hjælp af efterfølgende tilsynsforanstaltninger, når det kan dokumenteres, at en udbyder af digitale tjenester ikke opfylder kravene i artikel 16. Denne dokumentation kan indgives af en kompetent myndighed i en anden medlemsstat, hvor tjenesten leveres.

2. Med henblik på stk. 1 tillægges de kompetente myndigheder de fornødne beføjelser og midler til at pålægge udbydere af digitale tjenester at:

- a) forelægge de oplysninger, der er nødvendige for at vurdere sikkerheden af deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker

b) afhjælpe mangler i opfyldelsen af de krav, der er fastsat i artikel 16.

3. Hvis en udbyder af digitale tjenester har sit hjemsted eller en repræsentant i en medlemsstat, men dets net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder den kompetente myndighed i den medlemsstat, hvor hjemstedet eller repræsentanten befinder sig, og de kompetente myndigheder i de pågældende andre medlemsstater og bistår hinanden efter behov. En sådan bistand og et sådant samarbejde kan omfatte udveksling af oplysninger mellem de berørte kompetente myndigheder og anmodninger om at gennemføre de tilsynsforanstaltninger, der er omhandlet i stk. 2.

#### *Artikel 18*

### **Jurisdiktion og territorialitet**

1. Med henblik på dette direktiv anses en udbyder af digitale tjenester for at høre under den medlemsstats jurisdiktion, hvor den har sit hjemsted. En udbyder af digitale tjenester anses for at have sit hjemsted i en medlemsstat, hvis dens hovedkontor er placeret i den pågældende medlemsstat.

2. En udbyder af digitale tjenester, som ikke er etableret i Unionen, men som tilbyder tjenester som omhandlet i bilag III i Unionen, udpeger en repræsentant i Unionen. Repræsentanten skal være etableret i en af de medlemsstater, hvor tjenesterne tilbydes. En udbyder af digitale tjenester anses for at høre under den medlemsstats jurisdiktion, hvor repræsentanten er etableret.

3. Udpegelsen af en repræsentant af udbyderen af digitale tjenester berører ikke eventuelle retlige skridt mod selve udbyderen af digitale tjenester.

## **KAPITEL VI**

### **STANDARDISERING OG FRIVILLIG UNDERRETNING**

#### *Artikel 19*

### **Standardisering**

1. For at sikre en konvergerende gennemførelse af artikel 14, stk. 1 og 2, og artikel 16, stk. 1 og 2, tilskynder medlemsstaterne til at benytte europæiske eller internationalt anerkendte standarder og specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi.

2. ENISA udarbejder i samarbejde med medlemsstaterne vejledning og retningslinjer om de tekniske områder, der skal overvejes i forbindelse med stk. 1, samt om allerede eksisterende standarder, herunder medlemsstaternes nationale standarder, hvilket vil give mulighed for at dække disse områder.

#### *Artikel 20*

### **Frivillig underretning**

1. Med forbehold af artikel 3 kan enheder, som ikke er blevet identificeret som operatører af væsentlige tjenester og ikke er udbydere af digitale tjenester, på frivillig basis underrette om hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som de leverer.

2. Når medlemsstaterne behandler underretninger, handler de efter proceduren i artikel 14. Medlemsstaterne kan prioritere behandling af obligatoriske underretninger før frivillige underretninger. Frivillige underretninger behandles udelukkende, når en sådan behandling ikke udgør en uforholdsmæssig stor eller unødvendig byrde for de berørte medlemsstater.

Frivillig underretning må ikke medføre, at den underrettende enhed pålægges nogen forpligtelser, som den ikke ville være omfattet af, hvis den ikke havde indgivet denne underretning.

## **KAPITEL VII**



## AFSLUTTENDE BESTEMMELSER

### *Artikel 21*

#### **Sanktioner**

Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale regler, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger til at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaterne giver senest den 9. maj 2018 Kommissionen meddelelse om disse regler og foranstaltninger, og underretter den straks om alle senere ændringer, der berører dem.

### *Artikel 22*

#### **Udvalgsprocedure**

1. Kommissionen bistås af udvalget for sikkerhed i net- og informationssystemer. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

### *Artikel 23*

#### **Revision**

1. Senest den 9. maj 2019 forelægger Kommissionen Europa-Parlamentet og Rådet en rapport med en vurdering af ensartetheden i medlemsstaternes tilgange i forbindelse med identificeringen af operatører af væsentlige tjenester.

2. Kommissionen tager regelmæssigt dette direktivs funktion op til revision og forelægger en rapport for Europa-Parlamentet og Rådet. Til dette formål og med henblik på yderligere at fremme det strategiske og operationelle samarbejde tager Kommissionen højde for rapporterne fra samarbejdsgruppen og CSIRT-netværket om de erfaringer, der er gjort på strategisk og operationelt plan. I sin revision vurderer Kommissionen også listerne i bilag II og III samt ensartetheden i forbindelse med identificeringen af operatører af væsentlige tjenester og tjenester i de sektorer, der er omhandlet i bilag II. Den første rapport forelægges senest den 9. maj 2021.

### *Artikel 24*

#### **Overgangsforanstaltninger**

1. Uden at det berører artikel 25 og med henblik på at give medlemsstaterne flere muligheder for passende samarbejde under gennemførelsesperioden påbegynder samarbejdsgruppen og CSIRT-netværket deres opgaver, jf. henholdsvis artikel 11, stk. 3, og artikel 12, stk. 3, senest den 9. februar 2017.

2. I perioden fra den 9. februar 2017 til den 9. november 2018 og med henblik på at støtte medlemsstaterne i at anvende en ensartet tilgang, når operatører af væsentlige tjenester identificeres, drøfter samarbejdsgruppen processen, indholdet og typen af nationale foranstaltninger, som gør det muligt at identificere operatører af væsentlige tjenester inden for en bestemt sektor i overensstemmelse med kriterierne i artikel 5 og 6. Efter anmodning fra en medlemsstat drøfter samarbejdsgruppen også denne medlemsstats konkrete udkast til nationale foranstaltninger, som gør det muligt at identificere operatører af væsentlige tjenester inden for en bestemt sektor i overensstemmelse med kriterierne i artikel 5 og 6.

3. Senest den 9. februar 2017 og med henblik på denne artikel sikrer medlemsstaterne en passende repræsentation i samarbejdsgruppen og CSIRT-netværket.

### *Artikel 25*

### **Gennemførelse**

1. Medlemsstaterne vedtager og offentliggør senest den 9. maj 2018 de love og administrative bestemmelser, der er nødvendige for at efterkomme dette direktiv. De meddeler straks Kommissionen herom.

De anvender disse love og bestemmelser fra den 10. maj 2018.

Disse love og bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. Medlemsstaterne fastsætter de nærmere regler for henvisningen.

2. Medlemsstaterne meddeler Kommissionen teksten til de vigtigste nationale retsforskrifter, som de udsteder på det område, der er omfattet af dette direktiv.

#### *Artikel 26*

### **Ikrafttræden**

Dette direktiv træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

#### *Artikel 27*

### **Adressater**

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Strasbourg, den 6. juli 2016.

*På Europa-Parlamentets vegne*

**M. SCHULZ**

*Formand*

*På Rådets vegne*

**I. KORČOK**

*Formand*

- 1) EUT C 271 af 19.9.2013, s. 133.
- 2) Europa-Parlamentets holdning af 13.3.2014 (endnu ikke offentliggjort i EUT) og Rådets førstebehandlingsholdning af 17.5.2016 (endnu ikke offentliggjort i EUT). Europa-Parlamentets holdning af 6.7.2016 (endnu ikke offentliggjort i EUT).
- 14) Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre (EUT L 345 af 23.12.2008, s. 75).
- 15) Europa-Parlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA (EUT L 335 af 17.12.2011, s. 1).
- 16) Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).
- 17) Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).
- 18) Europa-Parlamentets og Rådets direktiv 2013/11/EU af 21. maj 2013 om alternativ tvistbilæggelse i forbindelse med tvister på forbrugerområdet og om ændring af forordning (EF) nr. 2006/2004 og direktiv 2009/22/EF (direktiv om ATB på forbrugerområdet) (EUT L 165 af 18.6.2013, s. 63).
- 19) Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

**Bilag I****KRAV TIL DE ENHEDER, DER HÅNDTERER IT-SIKKERHEDSHÆNDELSER (CSIRT'er),  
OG DERES OPGAVER**

Kravene til CSIRT'er og deres opgaver skal være tilstrækkeligt og klart defineret og understøttet af national politik og/eller regulering. De skal omfatte følgende:

- 1) Krav til CSIRT'er:
  - a) CSIRT'er skal sikre et højt tilgængelighedsniveau for deres kommunikationstjenester ved at undgå svage punkter («single points of failure») og for til enhver tid at have flere muligheder for at blive kontak- tet og til at kontakte andre. Desuden skal kommunikationskanalerne være tydeligt angivet og kendt af samarbejdspartnere.
  - b) CSIRT'ers lokaler og de underliggende informationssystemer skal være placeret i sikrede områder.
  - c) Driftskontinuitet:
    - i) CSIRT'er skal være udstyret med et passende system til at administrere og videresende anmodnin- ger, så overdragelser lettes
    - ii) CSIRT'er skal have tilstrækkeligt personale til at sikre tilgængelighed døgnet rundt
    - iii) CSIRT'er skal råde over en infrastruktur, hvis driftskontinuitet er sikret. Med henblik herpå skal redundante systemer og backuparbejdsområder være til rådighed
  - d) CSIRT'er skal, hvis de ønsker det, have mulighed for at deltage i internationale samarbejdsnetværk.
- 2) CSIRT'ers opgaver:
  - a) CSIRT'ers opgaver skal som minimum omfatte følgende:
    - i) monitorering af hændelser på nationalt plan
    - ii) tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om ri- sici og hændelser
    - iii) at reagere på hændelser
    - iv) udarbejdelse af dynamiske risiko- og hændelsesanalyser og situationsrapporter
    - v) deltagelse i CSIRT-netværket
  - b) CSIRT'er skal etablere et samarbejde med den private sektor.
  - c) For at lette samarbejdet fremmer CSIRT'er vedtagelse og anvendelse af fælles eller standardiseret praksis for:
    - i) procedurer for håndtering af hændelser og risici
    - ii) systemer til klassificering af hændelser, risici og oplysninger.

**TYPER AF ENHEDER MED HENBLIK PÅ ARTIKEL 4, NR. 4)**

Sektor		Delsektor		Type af enhed
1.	Energi	a)	Elektricitet	- Elektricitetsvirksomhed som defineret i artikel 2, nr. 35), i Europa-Parlamentets og Rådets direktiv 2009/72/EF <sup>1)</sup> , der varetager »forsyningen« som defineret i artikel 2, nr. 19), i nævnte direktiv
				- Distributionssystemoperatører som defineret i artikel 2, nr. 6), i direktiv 2009/72/EF
				- Transmissionssystemoperatører som defineret i artikel 2, nr. 4), i direktiv 2009/72/EF
				- Olierørledningsoperatør
		b)	Olie	Operatører af olieproduktion, raffinaderier og behandlingsanlæg, olielagre og olietransmission
		c)	Gas	- Operatører af olieproduktion, raffinaderier og behandlingsanlæg, olielagre og olietransmission
				- Forsyningsvirksomheder som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets direktiv 2009/73/EF <sup>2)</sup>
				- Distributionssystemoperatører som defineret i artikel 2, nr. 6), i direktiv 2009/73/EF
				- Transmissionssystemoperatører som defineret i artikel 2, nr. 4), i direktiv 2009/73/EF
				- Lagersystemoperatører som defineret i artikel 2, nr. 10), i direktiv 2009/73/EF

				- LNG-systemoperatører som defineret i artikel 2, nr. 12), i direktiv 2009/73/EF
				- Naturgasvirksomheder som defineret i artikel 2, nr. 1), i direktiv 2009/73/EF
				- Naturgasoperatør, raffinaderier og behandlingsanlæg
2.	Transport	a)	Lufttransport	- Luftfartsselskaber som defineret i artikel 3, nr. 4), i Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 <sup>3)</sup>
				- Lufthavnsdriftsorganer som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets direktiv 2009/12/EF <sup>4)</sup> , lufthavne som defineret i artikel 2, nr. 1), i nævnte direktiv, herunder de hovedlufthavne, der er anført i afsnit 2 i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 <sup>5)</sup> ; og enheder med tilknyttede anlæg i lufthavne
				- Trafikledelses- og kontroloperatører, der udøver flyvekontrolltjeneste som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 <sup>6)</sup>
		b)	Jernbanetransport	- Infrastrukturforvalter som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets direktiv 2012/34/EU <sup>7)</sup>
				- som defineret i artikel 3, nr. 1), i direktiv 2012/34/EU, herunder operatører af servicefaciliteter som defineret i artikel 3, nr. 12), i direktiv 2012/34/EU
		c)	Søfart	- Rederier, som udfører passager- og godstransport ad indre

				vandveje, i højsøfarvand eller kystnært farvand som defineret for søtransport i bilag I til Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 <sup>8)</sup> , bortset fra de enkelte fartøjer, som drives af disse rederier
				- Skibstrafiktjenesteoperatører som defineret i artikel 3, litra o), i Europa-Parlamentets og Rådets direktiv 2002/59/EF <sup>9)</sup>
				- Havnedriftsorganer som defineret i artikel 3, nr. 1), i Europa-Parlamentets og Rådets direktiv 2005/65/EF <sup>10)</sup> , herunder deres havnefaciliteter som defineret i artikel 2, nr. 11), i forordning (EF) nr. 725/2004; og enheder, der opererer anlæg og udstyr i havne
		d)	Vejtransport	- Vejmyndigheder som defineret i artikel 2, nr. 12), i Kommissionens delegerede forordning (EU) 2015/962 <sup>11)</sup> , og som er ansvarlige for trafikledelse
				- Operatører af intelligente transportsystemer som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets direktiv 2010/40/EU <sup>12)</sup>
3.	Bankvæsen			- Kreditinstitutter som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 <sup>13)</sup>
4.	Finansielle markedsinfrastrukturer			- Markedspladsoperatører som defineret i artikel 4, nr. 24), i Europa-Parlamentets og Rådets direktiv 2014/65/EU <sup>14)</sup>

				-	Central modpart (CCP) som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 <sup>15)</sup>
5.	Sundhedssektoren		Sundhedstjenestemiljøer (herunder hospitaler og private klinikker)	-	Sundhedstjenesteydere som defineret i artikel 3, litra g), i Europa-Parlamentets og Rådets direktiv 2011/24/EU <sup>16)</sup>
6.	Drikkevandsforsyning og distribution	Leverandør og distributør af »drikkevand« som defineret i artikel 2, nr. 1), litra a), i Rådets direktiv 98/83/EF <sup>17)</sup> bortset fra distributører, for hvem distribution af drikkevand kun er en del af deres generelle aktivitet med distribution af andre råvarer og varer, der ikke anses som væsentlige tjenester.			
7.	Digital infrastruktur	-	IXP'er		
		-	DNS-tjenesteudbydere		
		-	TLD-navneadministratorer		

- 1) Europa-Parlamentets og Rådets direktiv 2009/72/EF af 13. juli 2009 om fælles regler for det indre marked for elektricitet og om ophævelse af direktiv 2003/54/EF (EUT L 211 af 14.8.2009, s. 55).
- 2) Europa-Parlamentets og Rådets direktiv 2009/73/EF af 13. juli 2009 om fælles regler for det indre marked for naturgas og om ophævelse af direktiv 2003/55/EF (EUT L 211 af 14.8.2009, s. 94).
- 3) Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002 (EUT L 97 af 9.4.2008, s. 72).
- 4) Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002 (EUT L 97 af 9.4.2008, s. 72).
- 5) Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 af 11. december 2013 om Unionens retningslinjer for udvikling af det transeuropæiske transportnet og om ophævelse af afgørelse nr. 661/2010/EU (EUT L 348 af 20.12.2013, s. 1).
- 6) Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 af 10. marts 2004 om rammene for oprettelse af et fælles europæisk luftrum (»rammeforordningen«) (EUT L 96 af 31.3.2004, s. 1).
- 7) Europa-Parlamentets og Rådets direktiv 2012/34/EU af 21. november 2012 om oprettelse af et fælles europæisk jernbaneområde (EUT L 343 af 14.12.2012, s. 32).
- 8) Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 af 31. marts 2004 om bedre sikring af skibe og havnefaciliteter (EUT L 129 af 29.4.2004, s. 6).
- 9) Europa-Parlamentets og Rådets direktiv 2002/59/EF af 27. juni 2002 om oprettelse af et trafikovervågnings- og trafikinformationssystem for skibsfarten i Fællesskabet og om ophævelse af Rådets direktiv 93/75/EØF (EFT L 208 af 5.8.2002, s. 10).
- 10) Europa-Parlamentets og Rådets direktiv 2005/65/EF af 26. oktober 2005 om bedre havnesikring (EUT L 310 af 25.11.2005, s. 28).
- 11) Kommissionens delegerede forordning (EU) 2015/962 af 18. december 2014 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2010/40/EU for så vidt angår tilrådgivningsstillelse af EU-dækkende tidstro trafikinformationstjenester (EUT L 157 af 23.6.2015, s. 21).
- 12) Europa-Parlamentets og Rådets direktiv 2010/40/EU af 7. juli 2010 om rammene for indførelse af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportformer (EUT L 207 af 6.8.2010, s. 1).
- 13) Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1).
- 14) Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349).



- <sup>15)</sup> Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1).
- <sup>16)</sup> Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).
- <sup>17)</sup> Rådets direktiv 98/83/EF af 3. november 1998 om kvaliteten af drikkevand (EFT L 330 af 5.12.1998, s. 32).

**Bilag III****TYPER AF DIGITALE TJENESTER MED HENBLIK PÅ ARTIKEL 4, NR. 5)**

1. Onlinemarkedsplads
2. Onlinesøgemaskine
3. Cloud computing-tjeneste.