FOLKETINGSTIDENDE A

FOLKETINGET

Fremsat den 7. februar 2018 af erhvervsministeren (Brian Mikkelsen)

Forslag

til

Lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester[1)]

Kapitel 1

Anvendelsesområde og definitioner

§ 1. Loven finder anvendelse på operatører af væsentlige tjenester inden for digital infrastruktur og udbydere af digitale tjenester, jf. dog stk. 2.

Stk. 2. Loven finder ikke anvendelse på udbydere af digitale tjenester i form af mikrovirksomheder eller små virksomheder.

§ 2. I denne lov forstås ved:

1) Net- og informationssystem:
   a) Elektronisk kommunikationsnet i form af radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af tjenester,
   b) enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller
   c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.
2) 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.
3) Operatør af tjenester: En offentlig eller privat enhed etableret i Danmark, der leverer en DNS-tjeneste eller er administrator af et topdomænenavn.
4) Operatør af væsentlige tjenester: En offentlig eller privat enhed etableret i Danmark, der leverer en DNS-tjeneste eller er administrator af et topdomænenavn, og som opfylder kriterierne fastsat i § 3.
5) Digital tjeneste: Enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager, og som er af typen onlinemarkedsplads, onlinesøgemaskine eller cloud computing-tjeneste.
6) Udbyder af digitale tjenester: Enhver juridisk person, som udbyder en digital tjeneste, og som har hovedsæde eller en repræsentant i Danmark.
7) Hændelse: Enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.
8) Risiko: Enhver rimelig identificerbar omstændighed eller begivenhed, der har en potentiel negativ indvirkning på sikkerheden i net- og informationssystemer.
9) Repræsentant: Enhver fysisk eller juridisk person, der er etableret i EU, og som udtrykkeligt er udpeget til at handle på vegne af en udbyder af digitale tjenester, som ikke er etableret i EU.
10) Domænenavnesystem (DNS): Et hierarkisk opbygget navnesystem i et net, som behandler forespørgsler om domænenavne.
11) DNS-tjenesteudbyder: En enhed, som leverer DNS-tjenester på internettet.
12) Topdomænenavneadministrator: En enhed, som administrerer og driver registreringen af internetdomænenavne under et særligt topdomæne (TLD).
13) Onlinemarkedsplads: En digital tjeneste, som giver forbrugere eller erhvervsdrivende mulighed for at indgå aftaler om køb eller tjenester online med erhvervsdrivende enten på onlinemarkedspladsens websted el-

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

Erhvervsmin.,
Erhvervsstyrelsen, j.nr. 2018-2074

ler på et websted tilhørende en erhvervsdrivende, som anvender computing-tjenester, der udbydes af onlinemarkedspladsen.

14) Onlinesøgemaskine: En digital tjeneste, som giver brugerne mulighed for at foretage søgninger på 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.
15) Cloud computing-tjeneste: En digital tjeneste, som giver adgang til en skalerbar og elastisk pulje af delbare it-ressourcer.
16) Nationalt centralt kontaktpunkt: En national kompetent enhed med ansvar for at koordinere spørgsmål vedrørende sikkerheden i net- og informationssystemer samt grænseoverskridende samarbejde i EU herom.
17) CSIRT: En national it-beredskabsenhed, der håndterer hændelser, og som har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU.
18) Mikrovirksomheder og små virksomheder: Enheder, som opfylder definitionen som værende mikrovirksomheder eller små virksomheder i Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Kapitel 2

Operatører af væsentlige tjenester

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

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

Stk. 2. Erhvervsministeren udarbejder og opdaterer en liste over væsentlige tjenester.

Stk. 3. Erhvervsministeren kan fastsætte nærmere regler for afgrænsningen af kriterierne i stk. 1.

§ 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. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står mål med 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 væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester.

Stk. 3. Erhvervsministeren kan fastsætte nærmere regler om foranstaltninger efter stk. 1 og 2.

§ 5. Operatører af væsentlige tjenester skal hurtigst muligt underrette Erhvervsstyrelsen 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 Erhvervsstyrelsen og Center for Cybersikkerhed at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen.

Stk. 2. Med henblik på at fastlægge omfanget af en hændelses konsekvenser efter stk. 1, skal operatøren navnlig inddrage følgende kriterier:

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. Er en operatørs levering af en væsentlig tjeneste afhængig af en tredjepartsudbyder af digitale tjenester, skal operatøren underrette Erhvervsstyrelsen og Center for Cybersikkerhed om alle de væsentlige konsekvenser for den væsentlige tjenestes kontinuitet, som følger af en hændelse hos den pågældende udbyder.

Stk. 4. Erhvervsministeren kan fastsætte nærmere regler om underretning efter stk. 1 og 3, og om kriterierne for fastlæggelse af omfanget af en hændelses konsekvenser efter stk. 2.

§ 6. Erhvervsstyrelsen kan videregive oplysninger til Center for Cybersikkerhed om hændelser, der er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver som nationalt centralt kontaktpunkt og CSIRT.

Stk. 2. Erhvervsstyrelsen kan videregive relevante oplysninger til den underrettende operatør af væsentlige tjenester om opfølgningen på underretningen, herunder oplysninger der kan støtte en effektiv håndtering af hændelsen.

Stk. 3. Erhvervsstyrelsen kan efter høring af den underrettende operatør af væsentlige tjenester oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Kapitel 3

Udbydere af digitale tjenester

§ 7. En udbyder af en digital tjeneste, der ikke har hovedsæde i EU, men som tilbyder sin tjeneste i Danmark, skal udpege en repræsentant i Danmark eller i et andet EU-land, hvor tjenesten tilbydes.

§ 8. Udbydere af digitale tjenester skal identificere og træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene i forhold til sikkerheden i de net- og informationssystemer, som de anvender i forbindelse med tjenesten. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i mål med risikoen. Udbyderen skal i den forbindelse inddrage følgende elementer:

1) Sikkerheden i systemer og faciliteter.
2) Håndtering af hændelser.
3) Styring af driftskontinuitet.
4) Monitorering, audit og testning.
5) Overholdelse af internationale standarder.

Stk. 2. Udbydere af digitale tjenester skal træffe foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i deres net- og informationssystemer for at sikre kontinuiteten i disse tjenester.

Stk. 3. Erhvervsstyrelsen kan fastsætte nærmere regler om foranstaltninger efter stk. 1 og 2.

§ 9. Udbydere af digitale tjenester skal hurtigst muligt underrette Erhvervsstyrelsen og Center for Cybersikkerhed om enhver hændelse, der har betydelige konsekvenser for leveringen af deres tjeneste. Underretningen skal indeholde oplysninger, der gør det muligt for Erhvervsstyrelsen og Center for Cybersikkerhed at vurdere de eventuelle grænseoverskridende konsekvenser ved hændelsen, jf. dog stk. 3.

Stk. 2. Med henblik på at fastlægge, om en hændelses konsekvenser er betydelige, skal udbyderen navnlig inddrage følgende kriterier:

1) Antallet af brugere, der berøres af hændelsen, navnlig brugere, som er afhængige af tjenesten med henblik på levering af deres egne tjenester.
2) Hændelsens varighed.
3) Den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.
4) Omfanget af afbrydelsen af tjenestens funktion.
5) Omfanget af konsekvenserne for økonomiske og samfundsmæssige aktiviteter.

Stk. 3. Underretning efter stk. 1 skal kun ske, i det omfang udbyderen af digitale tjenester har adgang til relevante oplysninger, herunder oplysninger omfattet af stk. 2.

Stk. 4. Erhvervsstyrelsen kan fastsætte nærmere regler om underretning efter stk. 1 og 3, og om kriterierne for fastlæggelse af omfanget af en hændelses konsekvenser efter stk. 2.

§ 10. Erhvervsstyrelsen kan videregive oplysninger til Center for Cybersikkerhed om hændelser, der er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver som nationalt centralt kontaktpunkt og CSIRT.

Stk. 2. Erhvervsstyrelsen kan efter høring af udbyderen af digitale tjenester oplyse offentligheden om konkrete hændelser eller kræve, at udbyderen af digitale tjenester offentliggør det, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse i øvrigt er i offentlighedens interesse.

Kapitel 4

Kommunikation

§ 11. Erhvervsstyrelsen kan fastsætte regler om, at skriftlig kommunikation til og fra styrelsen om forhold, som er omfattet af denne lov eller af regler udstedt i medfør af denne lov, skal foregå digitalt.

Stk. 2. Erhvervsstyrelsen kan fastsætte nærmere regler om digital kommunikation, herunder om anvendelse af bestemte it-systemer, særlige digitale formater og digital signatur el.lign.

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

§ 12. Erhvervsstyrelsen kan fastsætte regler om, at styrelsen kan udstede afgørelser og andre dokumenter efter denne lov eller efter regler udstedt i medfør af denne lov uden underskrift, med maskinelt eller på tilsvarende måde gengivet underskrift eller under anvendelse af en teknik, der sikrer entydig identifikation af den, som har udstedt afgørelsen eller dokumentet. Sådanne afgørelser og dokumenter sidestilles med afgørelser og dokumenter med personlig underskrift.

§ 13. Hvor det efter denne lov eller regler udstedt i medfør af denne lov er krævet, at et dokument, som er udstedt af andre end Erhvervsstyrelsen, skal være underskrevet, kan dette krav opfyldes ved anvendelse af en teknik, der sikrer entydig identifikation af den, som har udstedt dokumentet, jf. dog stk. 2. Sådanne dokumenter sidestilles med dokumenter med personlig underskrift.

Stk. 2. Erhvervsstyrelsen kan fastsætte nærmere regler om fravigelse af underskriftskrav. Det kan herunder bestemmes, at krav om personlig underskrift ikke kan fraviges for visse typer af dokumenter.

Kapitel 5

Tilsyn, påbud, offentliggørelse og klage

§ 14. Erhvervsstyrelsen fører tilsyn med overholdelsen af denne lov og de regler, der er udstedt i medfør af loven.

Stk. 2. Erhvervsstyrelsen kan kræve, at operatører af tjenester og udbydere af digitale tjenester afgiver de oplysninger, der er nødvendige for styrelsens tilsyn efter denne lov.

Stk. 3. Erhvervsstyrelsen kan som led i sit tilsyn med operatører af væsentlige tjenester kræve dokumentation af operatørerne for den faktiske gennemførelse af sikkerhedspolitikker.

Stk. 4. Erhvervsstyrelsen kan som led i sit tilsyn udstede påbud til operatører af væsentlige tjenester og udbydere af digitale tjenester om at afhjælpe mangler i opfyldelsen af de krav, der fremgår af henholdsvis §§ 4-5 og §§ 7-9 og regler som fastsættes i medfør af § 4, stk. 3, § 5, stk. 4, § 8, stk. 3 eller § 9, stk. 4.

§ 15. Erhvervsstyrelsen offentliggør på sin hjemmeside helt eller delvis afgørelser efter § 14, stk. 4. Afgørelser vedrørende fysiske personer offentliggøres i anonymiseret form.

Stk. 2. Afgørelser vedrørende en juridisk person offentliggøres med identiteten på den juridiske person, medmindre offentliggørelsen af identiteten vil være til skade for en igangværende strafferetlig efterforskning eller offentliggørelsen vil forvolde uforholdsmæssig stor skade, fx for den juridiske person, afgørelsen vedrører, investorer eller andre.

Stk. 3. Anonymisering af identiteten på en juridisk person sker efter 2 år regnet fra og med datoen for offentliggørelse.

§ 16. Erhvervsstyrelsens afgørelser efter § 14, stk. 2-4, kan ikke indbringes for anden administrativ myndighed.

Kapitel 6

Straf

§ 17. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde den, der

1) undlader at efterkomme Erhvervsstyrelsens krav efter § 14, stk. 2 eller 3, eller
2) undlader at efterkomme Erhvervsstyrelsens påbud efter § 14, stk. 4.

Stk. 2. I regler, der udstedes i medfør af § 3, stk. 3, § 4, stk. 3, § 5, stk. 4, § 8, stk. 3 eller § 9, stk. 4, kan der fastsættes straf af bøde.

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

Kapitel 7

Ikrafttræden

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

Kapitel 8

Ændringer i anden lovgivning

§ 19. I lov om finansiel virksomhed jf. lovbekendtgørelse nr. 1140 af 26. september 2017, som bl.a. ændret ved § 1 i lov nr. 667 af 8. juni 2017, § 1 i lov nr. 1547 af 19. december 2017 og senest ved § 34 i lov nr. 1555 af 19. december 2017 foretages følgende ændringer:

1. I *fodnoten* til lovens titel ændres »og dele af Europa-Parlamentets og Rådets direktiv 2015/849/EU af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (4. hvidvaskdirektiv), EU-Tidende 2015, nr. L 141, side 73« til: »dele af Europa-Parlamentets og Rådets direktiv 2015/849/EU af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (4. hvidvaskdirektiv), EU-Tidende 2015, nr. L 141, side 73, og dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 (NIS-direktivet), EU-Tidende 2016, nr. L 194, side 1«

2. I *§ 71, stk. 2*, indsættes som *2. pkt.:*

»Finanstilsynet kan desuden fastsætte nærmere regler om hændelsesrapportering for de virksomheder der udpeges som operatører af væsentlige tjenester i medfør af § 307 a, herunder om at Finanstilsynet og Center for Cybersikkerhed underrettes ved en hændelse, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer.«

3. Efter afsnit VIII indsættes:

»Afsnit VIII a

Kapitel 18 a

Identifikation af operatører af væsentlige tjenester

§ 307 a. Finanstilsynet udpeger mindst hvert andet år de penge- og realkreditinstitutter, der er operatører af væsentlige tjenester.

Stk. 2. Finanstilsynet skal i forbindelse med udpegningen efter stk. 1, lægge vægt på, at

1) de tjenester, der leveres, er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,
2) leveringen af tjenesten afhænger af net- og informationssystemer, og
3) en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Stk. 3. Finanstilsynet kan fastsætte nærmere regler om udpegning af operatører af væsentlige tjenester og de kriterier Finanstilsynet kan lægge vægt på efter stk. 1 og 2. Finanstilsynet udarbejder en liste over tjenester, jf. stk. 2, nr. 1.«

4. I *§ 354, stk. 6*, indsættes som *nr. 44:*

»44) Center for Cybersikkerhed under forudsætning af at oplysningerne er nødvendige for centeret til at opfylde deres lovbestemte opgaver som nationalt centralt kontaktpunkt eller CSIRT.«

5. Efter § 354 g indsættes:

»§ 354 h. Finanstilsynet kan efter høring af den virksomhed, der underretter Finanstilsynet og Center for Cybersikkerhed om en hændelse, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, orientere offentligheden om hændelsen, hvis offentlighedens kendskab hertil er nødvendig for at forebygge eller håndtere en igangværende hændelse. Offentliggørelsen må ikke indeholde fortrolige oplysninger om kundeforhold eller oplysninger omfattet af § 30 i lov om offentlighed i forvaltningen. Offentliggørelsen må ikke indeholde fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den Europæiske Union, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse.«

§ 20. I lov om kapitalmarkeder, jf. lovbekendtgørelse nr. 12 af 8. januar 2018, foretages følgende ændringer:

1. I *fodnoten* til lovens titel ændres »dele af Europa-Parlamentets og Rådets direktiv 2013/50/EU af 22. oktober 2013, EU-Tidende 2013, nr. L 294, side 13, og Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 349« til: »dele af Europa-Parlamentets og Rådets direktiv 2013/50/EU af 22. oktober 2013, EU-Tidende 2013, nr. L 294, side 13, Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 349, og dele af Europa-Parlamentets

og Rådets direktiv 2016/1148/EU af 6. juli 2016, EU-Tidende 2016, nr. L 194, side 1«.

2. Efter § 58 indsættes i afsnit IV:

»Identifikation af operatører af væsentlige tjenester

§ 58 a. Finanstilsynet udpeger mindst hvert andet år de operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester.

Stk. 2. Finanstilsynet skal i forbindelse med udpegningen efter stk. 1, lægge vægt på, at

1) de tjenester, der leveres, er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,
2) leveringen af tjenesten afhænger af net- og informationssystemer, og
3) en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Stk. 3. Finanstilsynet kan fastsætte nærmere regler om udpegning af operatører af væsentlige tjenester og de kriterier Finanstilsynet kan lægge vægt på efter stk. 1 og 2, herunder fastsætte nærmere regler om hændelsesrapportering, herunder om at Finanstilsynet og Center for Cybersikkerhed underrettes ved en hændelse, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer. Finanstilsynet udarbejder en liste over tjenester, jf. stk. 2, nr. 1.«

1. I *§ 225, stk. 1,* indsættes som *nr. 17:*

»17) Center for Cybersikkerhed under forudsætning af, at oplysningerne er nødvendige for centeret til opfyldelse af dets lovbestemte opgaver som nationalt centralt kontaktpunkt eller CSIRT.«

2. Efter § 236 indsættes før overskriften før § 237:

»§ 236 a. Finanstilsynet kan efter høring af en operatør af en markedsplads eller centrale modpart (CCP), der underretter Finanstilsynet og Center for Cybersikkerhed om en hændelse, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, orientere offentligheden om hændelsen, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangværende hændelse. Offentliggørelsen må ikke indeholde fortrolige oplysninger om kundeforhold eller oplysninger omfattet af § 30 i lov om offentlighed i forvaltningen. Offentliggørelsen må ikke indeholde fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den Europæiske Union, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse.«

Kapitel 9

Territorial bestemmelse

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

Stk. 2. §§ 19 og 20 kan ved kongelig anordning helt eller delvist sættes i kraft for Færøerne og Grønland med de ændringer, som de henholdsvis færøske og grønlandske forhold tilsiger. Bestemmelserne kan endvidere sættes i kraft på forskellige tidspunkter.

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

2. Lovforslagets formål og baggrund

3. Lovforslagets hovedindhold

3.1. Det digitale område

3.1.1. Operatører af væsentlige tjenester

3.1.1.1. Gældende ret

3.1.1.2. NIS-direktivet

3.1.1.3. Erhvervsministeriets overvejelser og foreslåede ordning

3.1.2. Udbydere af digitale tjenester

3.1.2.1. Gældende ret

3.1.2.2. NIS-direktivet

3.1.2.3. Erhvervsministeriets overvejelser og foreslåede ordning

3.1.3. Tilsyn

3.1.3.1. Gældende ret

3.1.3.2. NIS-direktivet

3.1.3.3. Erhvervsministeriets overvejelser og foreslåede ordning

3.2. Det finansielle område

3.2.1. Identificering af operatører af væsentlige tjenester

3.2.1.1. Gældende ret

3.2.1.2. NIS-direktivet

3.2.1.3. Erhvervsministeriets overvejelser og foreslåede ordning

3.2.2. Indberetningskrav for operatører af væsentlige tjenester

3.2.2.1. Gældende ret

3.2.2.2. NIS-direktivet

3.2.2.3. Erhvervsministeriets overvejelser og foreslåede ordning

3.2.3. Videregivelse af oplysninger

3.2.3.1. Gældende ret

3.2.3.2. NIS-direktivet

3.2.3.3. Erhvervsministeriets overvejelser og foreslåede ordning

3.2.4. Offentliggørelse af hændelser

3.2.4.1. Gældende ret

3.2.4.2. NIS-direktivet

3.2.4.3. Erhvervsministeriets overvejelser og foreslåede ordning

4. Økonomiske og administrative konsekvenser for det offentlige

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

6. Administrative konsekvenser for borgere

7. Miljømæssige konsekvenser

8. Forholdet til EU-retten

9. Hørte myndigheder og organisationer m.v.

10. Sammenfattende skema

1. Indledning

IT-sikkerhedshændelser, såsom cyberangreb og nedbrud af it-systemer, udgør en alvorlig trussel mod samfundet, der i stigende grad er afhængig af digitale systemer. Omfanget, hyppigheden og konsekvenserne af sådanne hændelser er tiltagende. Rådet og Europa-Parlamentet har på den baggrund vedtaget direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (herefter NIS-direktivet), EU-Tidende 2016, nr. L 194, side 1.

Lovforslaget implementerer NIS-direktivet på Erhvervsministeriets område. Lovforslaget implementerer for det første de elementer i direktivet, der vedrører informationssikkerhed for domænenavnssystemer og visse digitale tjenester. For det andet implementerer lovforslaget NIS-direktivet på det finansielle område. Implementeringsfristen i NIS-direktivet er den 9. maj 2018. Loven foreslås derfor at træde i kraft den 10. maj 2018.

Med dette lovforslag indføres der krav til operatører af væsentlige tjenester inden for digital infrastruktur og udbydere af digitale tjenester, der i højere grad tager højde for samfundets afhængighed af sådanne tjenester, og afspejler det aktuelle trusselsbillede. Operatørerne og udbyderne skal træffe passende sikkerhedsforanstaltninger på baggrund af en vurdering af de risici, virksomheden konkret står over for. Endvidere foreslås der indført et krav om, at de omfattede operatører og udbydere skal underrette myndighederne om eventuelle hændelser, der har forstyrrende virkning på levering af de pågældende tjenester. Det er vigtigt for Erhvervsministeriet, at operatørerne eller udbyderne på området kun bliver underlagt proportionale krav, der ikke er unødvendigt byrdefulde, og at operatørerne eller udbyderne i videst muligt omfang, baseret på det aktuelle trusselsbillede, overlades et skøn til selv at beslutte indholdet af deres sikkerhedspolitikker.

For så vidt angår det finansielle område stilles der allerede i dag krav til it-sikkerhed i overensstemmelse med NIS-direktivets formål. Med lovforslaget foreslås derfor mindre lovændringer af lov om finansiel virksomhed og lov om kapitalmarkeder, med henblik på at sikre en direktivnær implementering af NIS-direktivet på Erhvervsministeriets område for så vidt angår pengeinstitutter, realkreditinstitutter, operatører af markedspladser og centrale modparter (CCP'er).

2. Lovforslagets formål og baggrund

Formålet med lovforslaget er at sikre et højt niveau for net- og informationssikkerhed inden for digital infrastruktur og for digitale tjenester med henblik på at skabe endnu mere robuste digitale systemer.

Den øgede digitalisering af det danske samfund indebærer, at net- og informationssikkerhed spiller en stadig mere afgørende rolle i samfundet. Det er i høj grad en forudsætning for de økonomiske og samfundsmæssige aktiviteter, at infrastrukturen for informations- og kommunikationsteknologi (IKT-infrastruktur) samt de digitale tjenester fungerer pålideligt og sikkert.

Erfaringerne viser, at omfanget, hyppigheden og konsekvenserne af hændelser er tiltagende og udgør en alvorlig trussel på det digitale område. Området er således i højere grad blevet et mål for forsætligt skadelige handlinger, som har til formål at ødelægge eller forstyrre driften af digitale systemer. Uanset om hændelserne er tilsigtede eller ej, kan forstyrrelser på det digitale område have alvorlige konsekvenser. En hændelse kan fx være et cyberangreb eller oversvømmelse af en operatørs eller udbyders serverrum, således at de digitale tjenester m.v. ikke fungerer. Hændelser kan fx hindre gennemførelsen af økonomiske aktiviteter, medføre betydelige finansielle tab og underminere brugernes tillid. Forhold der alle kan medvirke til at skabe skade på samfundsøkonomien.

På teleområdet er net- og informationssikkerhed reguleret gennem lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed med tilhørende bekendtgørelse. Derudover er andre dele af IKT-infrastrukturen samt digitale tjenester – bortset fra topdomænet ".dk" – ikke underlagt regulering på net- og informationssikkerhedsområdet. Der kan derfor være en risiko for, at andre dele af IKT-infrastrukturen samt digitale tjenester ikke på samme måde som i telesektoren er tilstrækkeligt beskyttet mod hændelser.

Lovforslaget har derfor til formål at sikre, at også andre aktører på det digitale område foretager de nødvendige organisatoriske og sikkerhedsmæssige foranstaltninger, der kan imødegå den stigende trussel på området.

Med lovforslaget foreslås der indført sikkerhedskrav for operatører af væsentlige tjenester inden for digital infrastruktur og udbydere af visse digitale tjenester. Operatører af væsentlige tjenester omfatter i dette lovforslag operatører af domænenavne- og topdomænenavnesystemer. Operatører af domænenavnesystemer medvirker til, at et internetopkald rutes rigtig ved at oversætte et domænenavn til en internetadresse (talkode), som internetnettet forstår. Operatører af topdomænenavne registrerer domænenavne under et topdomænenavn (fx ".dk", ".com" eller ".sport"). Udbydere af digitale tjenester omfatter onlinemarkedspladser, onlinesøgemaskiner og cloud computing-tjenester. Lovforslagets bestemmelser gælder ikke for udbydere af digitale tjenester, som er mikrovirksomheder og små virksomheder.

Lovforslaget regulerer ikke behandling af personoplysninger. Det fremgår i den forbindelse af NIS-direktivets artikel 2, at behandling af personoplysninger i henhold til NIS-direktivet udføres i overensstemmelse med direktiv 95/46/EF.

For så vidt angår det finansielle område, har lovforslaget til formål at sikre et højt niveau for net- og informationssikkerhed for så vidt angår de pengeinstitutter, realkreditinstitutter, operatører af markeder og centrale modparter (CCP'er), der karakteriseres som operatører af væsentlige tjenester, med henblik på at opnå en direktivnær implementering af NIS-direktivet.

3. Lovforslagets hovedindhold

3.1. Det digitale område

3.1.1. Operatører af væsentlige tjenester

3.1.1.1 Gældende ret

Operatører af væsentlige tjenester er på nuværende tidspunkt ikke underlagt en samlet regulering i forhold til net- og informationssikkerhed.

Administratorer af topdomænenavne, der særligt er tildelt Danmark eller på anden vis tilknyttet Danmark er i dag omfattet af lov om internetdomæner, jf. Lov nr. 164 af 26. februar 2014. I lovens §§ 19-22 er der fastsat bestemmelser om sikker og stabil drift af internetdomæner, som gælder for tildelingen af topdomænenavnet ".dk". Der er endvidere i bekendtgørelse om internetdomænet .dk, jf. bekendtgørelse nr. 1129 af 23. september 2015 i §§10-13, fastsat yderligere bestemmelser om sikkerheds- og tilgængelighedsforhold i den del af domænenavnssystemet, som er omfattet af ".dk". Bestemmelserne vedrører bl.a. krav til certificering efter sikkerhedsstandarder, krav til høj tilgængelighed til topdomænenavnet ".dk" og rapportering af nedbrud af domænenavnsservertjenesten. Det er Erhvervsstyrelsen, der fører tilsyn med overholdelsen af disse regler.

Andre topdomænenavne, der i dag er tildelt danske virksomheder, er derimod ikke omfattet af ovenstående regler om sikkerhedsniveauer m.v., idet disse topdomænenavne ikke er tildelt efter lov om internetdomæner. Tildelingen er derimod sket direkte til virksomhederne af den almennyttige non-profit organisation Internet Corporation for Assigned Names and Numbers (ICANN), der er etableret i Californien. Der er her tale om generiske topdomænenavne, som ikke er landespecifikke, fx ".com", ".org" og ".sport".

Operatører af domænenavnesystemer, som medvirker til at dirigere internettrafikken, er dertil heller ikke underlagt regulering i forhold til net- og informationssikkerhed.

3.1.1.2. NIS-direktivet

I henhold til NIS-direktivet skal hver EU-medlemsstat identificere operatører af væsentlige tjenester. Medlemsstaterne skal i forlængelse heraf udarbejde en liste over væsentlige tjenester inden for de omfattede sektorer, herunder digital infrastruktur. Listen over væsentlige tjenester skal opdateres regelmæssigt og samtidig bruges til at identificere operatører af væsentlige tjenester i det pågældende EU-land. I afgrænsningen af operatører vil derudover indgå om tjenesten er afhængig af net- og informationssystemer, og om en hændelse vil få væsentlig forstyrrende virkning for leveringen af den pågældende tjeneste.

NIS-direktivet fastsætter dertil, at medlemsstaterne skal sikre, at operatører af væsentlige tjenester træffer passende og forholdsmæssige foranstaltninger for at styre risiciene for sikkerheden i de net- og informationssystemer, de anvender som led i deres tjeneste. Foranstaltningerne skal både være af teknisk og organisatorisk karakter samt tage højde for det aktuelle teknologiske stadie med det formål at sikre et sikkerhedsniveau, der står mål med risikoen for hændelser. De pågældende virksomheder vil i forlængelse heraf skulle foretage en risikovurdering gennem hele livscyklussen for deres net- og informationssystemer, herunder i forhold til udarbejdelse af kravspecifikationer, udbud, konfigurering, drift og udfasning.

NIS-direktivet fastlægger desuden, at operatører af væsentlige tjenester, for at kunne opretholde kontinuiteten i deres tjenester, skal træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i de net- og informationssystemer, de anvender.

NIS-direktivet fastsætter derudover, at operatører af væsentlige tjenester hurtigst muligt skal foretage en underretning til myndighederne om hændelser, der har væsentlige konsekvenser for kontinuiteten af deres tjenester. Underretningen skal gøre myndighederne i stand til at vurdere, om der er behov for at underrette myndigheder i andre medlemsstater og offentligheden.

NIS-direktivet foreskriver endelig, at myndighederne i det land, hvor en hændelse indtræffer, skal orientere de relevante myndigheder i andre berørte medlemsstater om hændelser hos operatører af væsentlige tjenester, der har væsentlige konsekvenser for kontinuiteten i væsentlige tjenester i de pågældende medlemsstater. Orienteringen vil skulle ske under overholdelse af krav om fortrolighed og sikkerhed. Myndighederne kan endvidere efter høring af operatøren offentliggøre konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Kravene til operatører af væsentlige tjenester er i NIS-direktivet udtryk for minimumsharmonisering, og der vil være et nationalt spillerum for at fastsætte yderligere krav til operatørerne. Erhvervsministeriet vurderer dog, at der ikke er grundlag for at gå længere end de krav, der følger af NIS-direktivet.

3.1.1.3 Erhvervsministeriets overvejelser og foreslåede ordning

Lovforslaget gennemfører NIS-direktivets bestemmelser for operatører af væsentlige tjenester inden for digital infrastruktur på Erhvervsministeriets område.

Det foreslås, at erhvervsministeren får bemyndigelse til at fastsætte de nærmere kriterier for identifikationen af operatører af væsentlige tjenester samt til at udarbejde og regelmæssigt at opdatere en liste over væsentlige tjenester.

Det foreslås endvidere, at der indføres sikkerhedskrav til operatører af væsentlige tjenester. Sikkerhedskravene vil indeholde de overordnede forpligtelser for operatører til at træffe risikostyringsforanstaltninger og underrette myndighederne i tilfælde af hændelser. Lovforslaget lægger sig op ad ordlyden i NIS-direktivets bestemmelser og fastlægger dermed ikke yderligere nationale krav.

Lovforslaget indeholder dertil en hjemmel til i bekendtgørelsesform at fastsætte de nærmere regler for operatørernes sikkerheds- og underretningsforpligtelser. Hjemlen skal bruges til nærmere at fastlægge forpligtelserne bl.a. efter de vejledninger, der ventes at udstedes i EU-regi på området. Dertil vil bemyndigelsen skulle anvendes til nærmere at fastsætte, hvordan operatørerne skal indberette hændelser. Det er i forbindelse med udmøntningen af bemyndigelsen centralt for Erhvervsministeriet, at operatørerne kun bliver underlagt proportionale krav, herunder at der ikke sker en overimplementering af NIS-direktivets krav, og i det omfang det er muligt overlades et skøn til selv at beslutte indholdet i deres sikkerhedspolitikker.

Endvidere foreslås det, at Erhvervsstyrelsen kan videregive oplysninger om hændelser til Center for Cybersikkerhed under forudsætning af, at oplysningerne er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver som nationalt centralt kontaktpunkt og CSIRT (Computer Security Incident Response Team) i henhold til NIS-direktivet. Det nationale kontaktpunkt vil bl.a. i henhold til NIS-direktivet skulle orientere kontaktpunkter i andre medlemsstater om hændelser, der har væsentlige konsekvenser for kontinuiteten i de væsentlige tjenester, der udbydes i de pågældende lande. I henhold til direktivet skal hver medlemsstat endvidere udpege en såkaldt CSIRT, hvis rolle som minimum omfatter 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 dynamisk risiko- og hændelsesanalyser og situationsrapporter.

Det foreslås endelig, at Erhvervsstyrelsen får mulighed for, hvor det er relevant og efter høring af den pågældende operatør, at orientere offentligheden om hændelser. Center for Cybersikkerhed kan i koordination med Erhvervsstyrelsen orientere offentligheden om hændelser, der berører flere samfundsvigtige sektorer.

I det omfang, at der behandles personoplysninger i de pågældende net- og informationssystemer omfattet af lovforslaget, skal den til enhver tid gældende lovgivning om behandling af personoplysninger i øvrigt iagttages.

3.1.2. Udbydere af digitale tjenester

3.1.2.1. Gældende ret

Udbydere af digitale tjenester, som defineret i NIS-direktivet, er på nuværende tidspunkt ikke underlagt regulering i forhold til net- og informationssikkerhed.

3.1.2.2. NIS-direktivet

NIS-direktivet fastlægger lignende krav for udbydere af digitale tjenester som for operatører af væsentlige tjenester. Udbydere af digitale tjenester skal ligeledes træffe risikostyringsforanstaltninger og foranstaltninger, der forebygger og minimerer konsekvensen af eventuelle hændelser. Centralt for udbydernes opfyldelse af kravene vil også her være, at de pågældende virksomheder foretager en risikovurdering gennem hele livscyklussen for deres net- og informationssystemer. Mere specifikt følger det af NIS-direktivet, at de nævnte foranstaltninger skal adressere spørgsmål vedrørende sikkerhed i udbyderens systemer og faciliteter, håndtering af hændelser, styring af driftskontinuitet, monitorering, audit (kontrol) og testning samt overholdelse af internationale standarder. Disse elementer specificeres yderligere i Kommissionens gennemførelsesforordning 2018/151/EU af 30. januar 2018 om regler for anvendelsen af Europa-Parlamentets og Rådets direktiv 2016/1148/EU for så vidt angår yderligere specifikation af de elementer, som udbydere af digitale tjenester skal tage i betragtning for at styre risiciene i forhold til sikkerheden i net- og informationssystemer, og af kriterierne for bestemmelse af, om en hændelses konsekvenser er betydelige.

NIS-direktivet fastsætter ligeledes for udbydere af digitale tjenester en forpligtelse til hurtigst muligt at underrette myndighederne om enhver hændelse, der har betydelige konsekvenser for leveringen af deres tjeneste. I vurderingen af, om en hændelse har væsentlige konsekvenser, skal derudover antal brugere, varighed og geografisk udbredelse også inddrages omfanget af afbrydelsen af tjenestens funktion samt konsekvenserne for samfundsmæssige og økonomiske aktiviteter. Disse elementer er nærmere specificeret i Kommissionens gennemførelsesforordning 2018/151/EU af 30. januar 2018.

Hvis det vurderes relevant, skal myndighederne i det land, hvor en hændelse indtræffer endvidere i henhold til NIS-direktivet orientere de relevante myndigheder i andre berørte medlemsstater om hændelser hos udbydere af digitale tjenester. Myndighederne vil dertil også efter høring af udbyderen kunne offentliggøre konkrete hændelser eller kræve, at udbyderen gør dette, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse i øvrigt er i offentlighedens interesse. Medlemsstaterne vil i henhold til NIS-direktivet ikke kunne fastsætte yderligere sikkerhedskrav for udbydere, da NIS-direktivets bestemmelser er udtryk for totalharmonisering. Der vil dog kunne stilles yderligere krav under hensynstagen til rigets sikkerhed. Denne mulighed er dog ikke udnyttet i lovforslaget. Det følger endvidere af NIS-direktivets betragtninger, at der ikke skal stilles lige så høje sikkerhedskrav til udbydere af digitale tjenester som til operatører af væsentlige tjenester, hvilket skal ses i sammenhæng med, at hændelser i digitale tjenester ikke har lige så store konsekvenser for samfundet, som hændelser vil have inden for digital infrastruktur. I forlængelse heraf bør udbyderne overlades et større skøn til selv at fastlægge indholdet af deres informationssikkerhedspolitikker. De foranstaltninger, udbyderne skal træffe, skal endvidere være procesorienterede og risikobaserede og indebærer ikke en forpligtelse for udbyderne til at udforme deres IKT-produkter og -tjenester på en særlig måde.

3.1.2.3 Erhvervsministeriets overvejelser og foreslåede ordning

Lovforslaget gennemfører NIS-direktivets bestemmelser for udbydere af digitale tjenester på Erhvervsministeriets område.

Det foreslås, at der indføres sikkerhedskrav til udbydere af digitale tjenester.

Sikkerhedskravene vil indeholde de overordnede forpligtelser for udbydere til at træffe risikostyringsforanstaltninger og underrette myndighederne om hændelser. Lovforslaget lægger sig op ad ordlyden i NIS-direktivets bestemmelser, idet der inden for området for digitale tjenester er tale om totalharmonisering, og der fastlægges dermed ikke yderligere nationale krav.

Lovforslaget indeholder dertil en hjemmel til at fastsætte nærmere regler for udbydernes sikkerheds- og underretningsforpligtelser. Hjemlen vil skulle bruges til at gennemføre Kommissionens gennemførelsesretsakter, der nærmere specificerer indholdet af de elementer, der indgår i sikkerhedskravene til udbyderne af digitale tjenester. Det er her centralt for Erhvervsministeriet, at udbyderne kun bliver underlagt proportionale krav, der ikke indeholder unødvendige administrative byrder, og at der i videst muligt omfang overlades et skøn til udbyderne til selv at beslutte indholdet af deres sikkerhedspolitikker. Dette er i overensstemmelse med de ovennævnte overvejelser, der også fremgår af NIS-direktivets betragtninger, bl.a. betragtning nr. 44.

Endvidere foreslås det, at Erhvervsstyrelsen kan videregive oplysninger om hændelser til Center for Cybersikkerhed under forudsætning af, at oplysningerne er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver som nationalt centralt kontaktpunkt og CSIRT i henhold til NIS-direktivet. Det nationale kontaktpunkt vil bl.a. i henhold til NIS-direktivet skulle orientere kontaktpunkter i andre medlemsstater om hændelser, der har betydelige konsekvenser for leveringen af tjenester, der udbydes i de pågældende lande. I henhold til direktivet skal hver medlemsstat endvidere udpege en såkaldt CSIRT, hvis rolle som minimum omfatter 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 dynamisk risiko- og hændelsesanalyser og situationsrapporter.

Det foreslås endelig, at Erhvervsstyrelsen får mulighed for, hvor det er relevant og efter høring af den pågældende udbyder, at orientere offentligheden om hændelser. Center for Cybersikkerhed kan i koordination med Erhvervsstyrelsen orientere offentligheden om hændelser, der berører flere samfundsvigtige sektorer.

I det omfang, at der behandles personoplysninger i de pågældende net- og informationssystemer omfattet af lovforslaget, skal den til enhver tid gældende lovgivning om behandling af personoplysninger i øvrigt iagttages.

3.1.3. Tilsyn

3.1.3.1. Gældende ret

Operatører af væsentlige tjenester inden for digital infrastruktur og udbydere af digitale tjenester er på nuværende tidspunkt ikke underlagt en samlet regulering i forhold til net- og informationssikkerhed.

Administratorer af topdomænenavne, der særligt er tildelt Danmark eller på anden vis tilknyttet Danmark er i dag omfattet af lov om internetdomæner (Lov nr. 164 af 26. februar 2014). Erhvervsstyrelsen er tilsynsmyndighed i forhold til denne regulering og kan i henhold til lovens § 37 udstede påbud om overholdelse af bestemmelser og vilkår til de omfattede operatører. I henhold til § 41, stk. 1, kan Erhvervsstyrelsen kræve af de omfattede administratorer enhver oplysning og ethvert materiale, som styrelsen skønner relevant i forbindelse med administration af loven og tilsynet hermed. Styrelsen kan endvidere indhente oplysningerne hos operatøren med henblik på offentliggørelse af statistik over bl.a. det samlede antal registrerede domænenavne og antal klagesager, jf. § 41, stk. 3. Endelig kan Erhvervsstyrelsen efter § 45 pålægge de omfattede administratorer tvangsbøder og efter § 46 tilbagekalde tilladelser tildelt til administratorer. Lov om internetdomæner og tilhørende bekendtgørelse vil ikke blive ændret med dette lovforslag.

3.1.3.2. NIS-direktivet

Lovforslaget gennemfører NIS-direktivets bestemmelser om offentliggørelse og tilsyn på Erhvervsministeriets område.

NIS-direktivet foreskriver, at medlemsstaterne skal sikre, at de kompetente myndigheder griber ind over for operatører og udbydere, der ikke opfylder deres forpligtelser. Myndighederne vil i forlængelse heraf skulle kunne pålægge operatørerne og udbyderne, at de forelægger de nødvendige oplysninger til brug for myndighedernes tilsyn, og at operatørerne og udbyderne afhjælper eventuelle mangler. For udbydere af digitale tjenester følger det af NIS-direktivet, at der skal være tale om et reaktivt tilsyn, hvilket skal ses i sammenhæng med, at hændelser for udbydere af digitale tjenester ikke vil have samme samfundsmæssige konsekvenser som ved hændelser hos operatører af væsentlige tjenester.

3.1.3.3. Erhvervsministeriets overvejelser og foreslåede ordning

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

Erhvervsstyrelsen vil som led i sit tilsyn overordnet få adgang til at kræve oplysninger fra operatører af væsentlige tjenester og udbydere af digitale tjenester, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer. Styrelsen vil endvidere få mulighed for at udstede påbud til operatører og udbydere om, at de fx skal afhjælpe mangler i deres efterlevelse af lovens bestemmelser.

Det foreslås derudover, at der i overensstemmelse med NIS-direktivets bestemmelser anlægges et mere aktivt tilsyn

over for operatører af væsentlige tjenester end udbydere af digitale tjenester. Således foreslås det, at Erhvervsstyrelsen som led i sit tilsyn af egen drift kan rette henvendelse til operatører af væsentlige tjenester med henblik på kontrol af operatørernes efterlevelse af loven. Forskellen skal ses i sammenhæng med, at hændelser i digitale tjenester ikke har lige så store konsekvenser for samfundet, som hændelser vil have inden for digital infrastruktur. I forlængelse heraf foreslås, at Erhvervsstyrelsen som led i sit tilsyn med operatører får mulighed for at kræve dokumentation af operatører for den faktiske gennemførelse af sikkerhedspolitikker.

For udbydere af digitale tjenester vil tilsynet i overensstemmelse med NIS-direktivet være reaktivt og baseret på dokumenteret manglende overholdelse af lovgivningens krav fra fx brugere og andre myndigheder, herunder myndigheder i andre lande.

Med lovforslaget indføres endelig, at Erhvervsstyrelsen efter høring af de pågældende operatører og udbydere har mulighed for at offentliggøre de afgørelser, som styrelsen træffer som led i sit tilsyn under hensyntagen til bl.a. persondatabeskyttelse og strafferetlig efterforskning.

Forslaget om offentliggørelse af oplysninger om hændelser og afgørelser, som ovenfor beskrevet, er udarbejdet med baggrund i de anbefalinger, som fremgår af Justitsministeriets betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser m.v. I betænkningen anbefales det, at der inden indførelse af ordninger med systematisk offentliggørelse af oplysning om kontrolresultater, afgørelser m.v. på internettet i ikke-anonymiseret form foretages en vurdering af det konkrete behov for offentliggørelse, om offentliggørelse kan forventes konkret at være særligt indgribende for personen, om der er tungtvejende samfundsmæssige hensyn bag offentliggørelsesordningen, om offentliggørelse strider mod de gældende databeskyttelsesretlige regler og de almindelige regler om tavshedspligt, og om der af retssikkerhedsmæssige grunde er opstillet administrative regler for forvaltningsmyndighedens behandling af de enkelte sager.

Den offentlige og private sektor er – indtil den 24. maj 2018 – omfattet af Lov nr. 429 af 31. maj 2000 med senere ændringer (herefter Persondataloven) og tilhørende bekendtgørelser, når der behandles personoplysninger. Persondataloven gennemfører databeskyttelsesdirektivet, som ophæves pr. 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. forslagets § 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, der regulerer området for behandling af personoplysninger.

Nærværende lovforslag indebærer dog, at oplysninger vedrørende fysiske personer altid vil blive offentliggjort i anonymiseret form. Der vil derfor som udgangspunkt ikke blive givet personoplysninger til offentligheden, hvorfor disse afgørelser ikke vil være reguleret af de gældende databeskyttelsesretlige regler. Afgørelser vedrørende en juridisk person offentliggøres med identiteten på den juridiske person, medmindre offentliggørelsen af identiteten vil være til skade for en igangværende strafferetlig efterforskning eller offentliggørelsen vil forvolde uforholdsmæssig stor skade, fx for den juridiske person, afgørelsen vedrører, investorer eller andre. Det vil således være Erhvervsstyrelsens vurdering, om det er nødvendigt for at forebygge eller håndtere en igangværende hændelse at offentliggøre navnet på den berørte virksomhed, eller om det samme resultat kan nås med en anonymiseret offentliggørelse, som alene omfatter den konkrete hændelse.

En offentliggørelse vil ske efter høring af operatøren, og Erhvervsstyrelsen vil foretage en afvejning af på den ene side offentlighedens interesse i at blive informeret om trusler og på den anden side mulig kommerciel skade samt skade for omdømmet for den pågældende operatør. Offentliggørelsen må dog ikke indeholde fortrolige oplysninger omfattet af § 27, stk. 1 i forvaltningsloven. Det vil særligt være i offentlighedens interesse at få oplysninger om en hændelse, som kan have betydning for at forebygge en gentagelse af hændelsen eller kan bidrage i forbindelse af håndtering af en igangværende hændelse.

3.2. Det finansielle område

3.2.1. Identificering af operatører af væsentlige tjenester

3.2.1.1. Gældende ret

I medfør af lov om finansiel virksomhed § 308 udpeger Finanstilsynet hvert år de systemisk vigtige finansielle institutter (SIFI) i Danmark. Et pengeinstitut, et realkreditinstitut og et fondsmæglerselskab I, hvis fondsmæglerselskabet I har tilladelse til at udøve de aktiviteter, der er nævnt i bilag 4, afsnit A, nr. 3 og 6, der er omfattet af Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber, udpeges som et systemisk vigtigt finansielt institut (SIFI), hvis det i 2 på hinanden følgende år, enten har en balance, der udgør mere end 6,5 pct. af Danmarks bruttonationalprodukt, eller hvis instituttets udlån i Danmark udgør mere end 5 pct. af de danske penge- og realkreditinstitutters samlede udlån i Danmark, eller hvis instituttets indlån i Danmark udgør mere end 5 pct. af de danske pengeinstitutters samlede indlån i Danmark.

3.2.1.2. NIS-direktivet

Det følger af direktivets artikel 5, stk. 1, at medlemsstaterne skal føre en liste over operatører af væsentlige tjenester, der er etableret for hver sektor og delsektor, som er omhandlet i direktivets bilag II. Denne identificering skal ajourføres mindst hvert andet år.

For så vidt angår den finansielle sektor omhandler direktivets bilag II sektorerne bankvæsen og finansielle markedsinfrastrukturer. Typen af enheder i disse sektorer er kreditinstitutter, operatører af markedspladser og centrale modparter (CCP), jf. NIS-direktivets bilag II.

Det følger endvidere af direktivets artikel 5, stk. 2, at ved identificering af operatører af væsentlige tjenester, skal der lægges vægt på følgende tre kriterier. Der skal være tale om en enhed, der leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter. Derudover skal leveringen af denne tjeneste afhænge af net- og informationssystemer. Som det sidste kriterie følger det af direktivet, at en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste. Ved vurderingen af om en hændelse er væsentlig forstyrrende, vil der bl.a. skulle lægges vægt på det antal af brugere der påvirkes, samt de konsekvenser en hændelse kan have i omfang og varighed på økonomiske og samfundsmæssige aktiviteter m.v., jf. direktivets artikel 6, stk. 1.

Direktivet er et minimumsharmoniseringsdirektiv, og der vil dermed være et nationalt spillerum for at fastsætte yderligere krav til operatørerne af væsentlige tjenester.

3.2.1.3. Erhvervsministeriets overvejelser og den foreslåede ordning

Det følger af NIS-direktivets bilag II, at kreditinstitutter, operatører af markedspladser og centrale modparter (CCP'er), er omfattet af NIS-direktivet. Det følger endvidere af direktivets artikel 5, stk. 2, at medlemsstaterne mindst hvert andet år skal udpege de kreditinstitutter, operatører af markedspladser og centrale modparter (CCP'er), som kan identificeres som operatører af væsentlige tjenester.

Et kreditinstitut er en virksomhed, hvis aktivitet består i fra offentligheden at modtage indlån eller andre midler, som skal tilbagebetales, samt i at yde lån for egen regning, jf. lov om finansiel virksomhed § 5, stk. 1, nr. 2. Det betyder, at et kreditinstitut både kan være et penge- og et realkreditinstitut.

Finanstilsynet udpeger i dag efter § 308 de pengeinstitutter, realkreditinstitutter og fondsmæglerselskaber, som er systemisk vigtige (SIFI).

For så vidt angår identificering af væsentlige tjenester på det finansielle område, fremgår det af NIS-direktivets præambel nr. 28, at med henblik på at fastslå, hvorvidt en hændelse ville have væsentlig forstyrrende virkning på leveringen af en væsentlig tjeneste, bør medlemsstaterne i tillæg til de tværsektorielle forhold også tage højde for sektorspecifikke forhold. Det fremgår endvidere af direktivet, at for så vidt angår det finansielle område, skal der tages hensyn til de pågældende virksomheders systemiske betydning baseret på de samlede aktiver eller de samlede aktiver i forhold til BNP. Det særlige krav til det finansielle område hænger i høj grad sammen med de samme kriterier, som i dag anvendes til udpegning af en SIFI.

En SIFI er et institut, hvis sammenbrud eller vanskeligheder rummer risiko for systemiske konsekvenser. Systemisk risiko er risiko for forstyrrelse af det finansielle system, som kan få alvorlige negative konsekvenser for det finansielle system og realøkonomien.

En SIFI udpeges på baggrund af størrelse, betydning for unionens eller en relevant medlemsstats økonomi, betydningen af grænseoverskridende aktiviteter og instituttets eller koncernens sammen-kobling med det finansielle system.

En SIFI måles på, at instituttets balance udgør mere end 6,5 pct. af Danmarks bruttonationalprodukt, at instituttets udlån i Danmark udgør mere end 5 pct. af de danske penge- og realkreditinstitutters samlede udlån i Danmark, og at instituttets indlån i Danmark udgør mere end 5 pct. af de danske pengeinstitutters samlede indlån i Danmark.

Der ses således at være en vis lighed mellem kriterierne for udpegning af væsentlige operatører inden for det finansielle område, og udpegningen af en SIFI.

Med lovforslaget sikres en direktivnær implementering af NIS-direktivet. Det foreslås på den baggrund at indføre en ny § 307 a i lov om finansiel virksomhed og en ny § 58 a i lov om kapitalmarkeder, hvorefter Finanstilsynet mindst hvert andet år udpeger de penge- og realkreditinstitutter samt de operatører af markedspladser og centrale modparter (CCP'ere), der er operatører af væsentlige tjenester. I den forbindelse skal Finanstilsynet lægge vægt på, at de tjenester som virksomhederne leverer, er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af tjenesterne afhænger af net- og informationssystemer, og at en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesten. Med en hændelse forstås enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.

Det foreslås endvidere, at Finanstilsynet kan fastsætte nærmere regler om kravene til identifikationen af operatører af væsentlige tjenester, herunder fastsætte nærmere regler om krav om underretning af Finanstilsynet og Center for Cybersikkerhed som nationalt centralt kontaktpunkt eller CSIRT ved en hændelse, jf. nærmere herom under pkt. 3.2.2. Derudover foreslås det, at Finanstilsynet får hjemmel til at udarbejde en liste over tjenester, der er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

Det forventes, at eftersom kriterierne for udpegning af operatører af væsentlige tjenester svarer til kriterierne for udpegning af SIFI'er efter § 308 i lov om finansiel virksomhed, vil de institutter, der udpeges som SIFI'er, tillige blive udpeget som operatører af væsentlige tjenester i NIS-direktivets forstand. Men ved at have en selvstændig udpegningsbestemmelse i § 307 a i lov om finansiel virksomhed, vurderes bestemmelsen at være fremtidssikret, såfremt der på et tidspunkt vurderes at være operatører i den finansielle sek-

tor, som vurderes at være væsentlige, men dog ikke vurderes at være en SIFI.

3.2.2. Indberetningskrav for operatører af væsentlige tjenester

3.2.2.1. Gældende ret

For så vidt angår penge- og realkreditinstitutter, følger det af § 71, stk. 1, i lov om finansiel virksomhed, at en finansiel virksomhed, en finansiel holdingvirksomhed og en forsikringsholdingvirksomhed skal have effektive former for virksomhedsstyring, herunder bl.a. betryggende kontrol- og sikringsforanstaltninger på it-området.

Det følger videre af § 71, stk. 2, at Finanstilsynet kan fastsætte nærmere regler om de foranstaltninger, som en finansiel virksomhed, en finansiel holdingvirksomhed og en forsikringsholdingvirksomhed skal træffe for at have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger på it-området. Denne bemyndigelse er bl.a. udnyttet ved bekendtgørelse nr. 1026 af 30. juni 2016 om ledelse og styring af pengeinstitutter m.fl. (herefter kaldet ledelsesbekendtgørelsen), hvoraf bekendtgørelsens bilag 5 blandt andet stiller nærmere krav til it-sikkerhed.

Det følger bl.a. af bekendtgørelsens bilag 5, at bestyrelsen skal beslutte en it-sikkerhedspolitik for virksomheden, som ud fra den ønskede risikoprofil på it-området skal indeholde en overordnet stillingtagen til alle væsentlige forhold vedrørende it-sikkerheden. Hvad der er væsentligt, afhænger bl.a. af virksomhedens størrelse samt omfanget og kompleksiteten af virksomhedens it-anvendelse.

Der følger ikke af ledelsesbekendtgørelsen et regulatorisk krav om indberetning af hændelser, men det skal fremhæves, at hændelsesrapportering er en væsentlig del af det løbende tilsyn og herunder en del af, at have effektive former for virksomhedsstyring. Finanstilsynet har som vejledning for de omfattede virksomheder beskrevet på sin hjemmeside, hvornår Finanstilsynet forventer at blive orienteret.

Det er i dag som udgangspunkt virksomheden selv, som vurderer, hvornår en hændelse er væsentlig. Dog er der nogle særlige situationer, hvor Finanstilsynet typisk bør orienteres. Det kan fx være, når hændelsen har potentiale til at udvikle sig til en katastrofesituation, der involverer gældende kriseberedskab, når hændelsen påvirker/kan påvirke den kritiske danske betalingsinfrastruktur eller komponenter heraf eller når hændelsen kan give anledning til politianmeldelse.

For så vidt angår operatører af markedspladser følger det af § 71, stk. 1, i lov om kapitalmarkeder, at en operatør af et reguleret marked er ansvarlig for, at det pågældende marked drives på en betryggende og hensigtsmæssig måde. Videre følger det af stk. 2, nr. 2, at en operatør skal kunne styre risici, som operatøren og markedet udsættes for, herunder kunne påvise alle væsentlige risici for markedets drift og indføre effektive foranstaltninger til at mindske disse risici. Det følger videre af stk. 2, nr. 3, at en operatør skal sikre en ordentlig forvaltning af den tekniske funktion af markedspladsens systemer, herunder etablere effektive nødssystemer.

Det følger endvidere, af § 81 i lov om kapitalmarkeder, at en operatør af et reguleret marked hurtigst muligt skal underrette Finanstilsynet, hvis operatøren bliver bekendt med eller har formodning om systemfejl i forbindelse med et finansielt instrument.

Derudover følger det af § 89, stk. 1, i lov om kapitalmarkeder, at en operatør af en multilateral handelsfacilitet (MHF) eller en organiseret handelsfacilitet (OHF) er ansvarlig for, at det pågældende marked drives på en betryggende og hensigtsmæssig måde. Af § 89, stk. 2, nr. 3, fremgår det videre, at operatøren skal sikre en ordentlig forvaltning af facilitetens tekniske drift, herunder etablere effektive nødsystemer.

Der findes ikke centrale modparter (CCP'er) i Danmark ved lovforslagets fremsættelse. En central modpart skal have en tilladelse og er underlagt tilsyn i henhold til Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 (EMIR-forordningen), som suppleres af tekniske standarder.

Ifølge artikel 26, stk. 6, i EMIR-forordningen skal en central modpart (CCP) have IT-systemer, der er egnede til at håndtere kompleksiteten, variationen og typen af serviceydelser, som den centrale modpart (CCP'en) udbyder. Dette med henblik på at sikre en høj IT-sikkerhed, integritet og fortrolighed omkring den data, som den centrale modpart (CCP'en) håndterer.

3.2.2.2. NIS-direktivet

I medfør af NIS-direktivet skal medlemsstaterne sikre, at operatører af væsentlige tjenester træffer passende og forholdsmæssige foranstaltninger for at styre risiciene for sikkerheden i de net- og informationssystemer, de anvender som led i deres tjeneste. Med sikkerhed i net- og informationssystemer forstås net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer. Foranstaltningerne skal både være af teknisk og organisatorisk karakter samt tage højde for det aktuelle teknologiske stade med det formål at sikre et sikkerhedsniveau, der står mål med risikoen for hændelser.

I medfør af NIS-direktivet skal operatører af væsentlige tjenester, for at kunne opretholde kontinuiteten i deres tjenester, træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i de net- og informationssystemer, de anvender.

Direktivet fastsætter derudover, at operatører af væsentlige tjenester hurtigst muligt skal foretage en underretning til de kompetente myndigheder eller CSIRT om hændelser, der har væsentlige konsekvenser for kontinuiteten af deres tjenester, jf. artikel 14, stk. 3. Underretningen skal gøre myndighederne i stand til at vurdere, om der er behov for at un-

derrette kompetente myndigheder i andre medlemsstater og offentligheden.

Artikel 9 i direktivet fastsætter krav om, at hver medlemsstat udpeger en såkaldt CSIRT, hvis rolle er nærmere defineret under pkt. 3.2.3.2. I medfør af artikel 10, stk. 2, skal medlemsstaterne sikre, at enten de kompetente myndigheder eller CSIRT'erne modtager underretning om hændelser, som har væsentlige konsekvenser for kontinuiteten af de tjenester, som de udpegede operatører af væsentlige tjenester leverer. I det omfang en CSIRT ikke modtager underretninger om hændelser, skal CSIRT'erne i stedet have oplysninger herom fra den kompetente myndighed.

Direktivet foreskriver endelig, at de kompetente myndigheder skal kunne orientere myndighederne i andre berørte medlemsstater om hændelser hos operatører af væsentlige tjenester, der har væsentlige konsekvenser for kontinuiteten i væsentlige tjenester i de pågældende medlemsstater. Orienteringen vil skulle ske under overholdelse af krav om fortrolighed og sikkerhed.

3.2.2.3. Erhvervsministeriets overvejelser og den foreslåede ordning

For så vidt angår kreditinstitutter, det vil sige penge- og realkreditinstitutter, gælder der allerede i dag en række krav til de foranstaltninger, som en finansiel virksomhed, skal træffe for at have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger på it-området. Disse krav fastsættes nærmere af Finanstilsynet i bekendtgørelse nr. 1026 af 30. juni 2016 om ledelse og styring af pengeinstitutter m.fl. (herefter ledelsesbekendtgørelsen) i medfør af lov om finansiel virksomhed § 71, stk. 2.

For så vidt angår operatører af markedspladser og centrale modparter (CCP'er) gælder der i medfør af lov om kapitalmarkeder og EMIR-forordningen også en række krav for disse virksomheder i forhold til risikostyring og sikkerhedsforanstaltninger på it-området.

Der gælder ikke i dag et regulatorisk krav om indberetning af hændelser for kreditinstitutter, men hændelsesrapportering er en væsentlig del af det løbende tilsyn. Det er i dag som udgangspunkt virksomheden selv, som vurderer, hvornår en hændelse er væsentlig. Finanstilsynet har som vejledning for de omfattede virksomheder beskrevet på sin hjemmeside, hvornår Finanstilsynet forventer at blive orienteret.

Det vurderes derfor at være mest hensigtsmæssigt, at der i ledelsesbekendtgørelsen indsættes en bestemmelse om, at operatører af væsentlige tjenester, skal foretage hændelsesunderretning både til Finanstilsynet og Center for Cybersikkerhed, der forventes at blive udpeget som CSIRT, jf. nærmere herom under pkt. 3.2.3.3.

For så vidt angår operatører af markedspladser og centrale modparter (CCP'ere) gælder i dag alene et underretningskrav i § 81 i lov om kapitalmarkeder, hvorefter en operatør af markedspladser skal underrette Finanstilsynet om systemfejl i forbindelse med et finansielt instrument. Der gælder ikke regler for de centrale modparter (CCP'ere), da en central modpart skal have en tilladelse og er underlagt tilsyn i henhold til Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 (EMIR-forordningen), som suppleres af tekniske standarder.

Det vurderes derfor at være mest hensigtsmæssigt, at der indsættes en hjemmel til at kunne udarbejde en bekendtgørelse, hvori der indsættes en bestemmelse om, at de operatører af markedspladser og centrale modparter (CCP'ere), der udpeges til at være væsentlige operatører, skal underrette Finanstilsynet og Center for Cybersikkerhed om hændelser.

Lovforslaget gennemfører NIS-direktivets bestemmelser for operatører af væsentlige tjenester på det finansielle område på Erhvervsministeriets område for så vidt angår indberetningspligt.

Med henblik på en direktivnær implementering af NIS-direktivet foreslås det, at Finanstilsynet i lov om finansiel virksomhed § 71, stk. 2, bemyndiges til også at kunne fastsætte nærmere regler for underretning om hændelsesrapportering ved eventuelle hændelser. Dermed vil Finanstilsynet i ledelsesbekendtgørelsen kunne fastsætte nærmere krav til indberetning fra de kreditinstitutter, der er operatører af væsentlige tjenester, når der er tale om hændelser, der har væsentlige konsekvenser for kontinuiteten af tjenester, og som er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

For så vidt angår operatører af markedspladser og centrale modparter (CCP'er) foreslås det ligeledes, at Finanstilsynet kan fastsætte nærmere regler i en bekendtgørelse om underretning af en hændelse hos en operatør af markedspladser eller en central modpart (CCP), der er operatører af væsentlige tjenester, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som leveres.

I medfør af lovforslaget vil underretning skulle ske til både Finanstilsynet og Center for Cybersikkerhed i medfør af deres rolle som CSIRT. Det skal i den forbindelse bemærkes, at der forventes etableret en fælles indberetningsløsning – fx gennem en fælles portal på virk.dk – hvorigennem alle operatører omfattet af NIS-direktivet vil kunne indberette. Med denne fælles indberetningsløsning forventes en afrapportering til både Finanstilsynet og Center for Cybersikkerhed dermed ikke at have økonomiske konsekvenser for de enkelte omfattede virksomheder.

3.2.3. Videregivelse af oplysninger

3.2.3.1. Gældende ret

I medfør af § 354, stk. 1, i lov om finansiel virksomhed og § 224 i lov om kapitalmarkeder, er Finanstilsynets ansatte underlagt en særlig tavshedspligt. Finanstilsynets ansatte er således under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger.

Finanstilsynet kan dog i visse lovbestemte tilfælde videregive fortrolige oplysninger til bestemte modtagere i medfør af § 354, stk. 6, i lov om finansiel virksomhed og § 225 i lov om kapitalmarkeder.

Finanstilsynet kan dog ikke i dag videregive oplysninger til Center for Cybersikkerhed i medfør af lov om finansiel virksomhed eller lov om kapitalmarkeder.

Endelig følger det af § 354, stk. 8, i lov om finansiel og § 229 i lov om kapitalmarkeder, at enhver der modtager fortrolige oplysninger fra Finanstilsynet, bliver underlagt den samme skærpede tavshedspligt.

3.2.3.2. NIS-direktivet

NIS-direktivet indeholder krav om udpegning af kompetente myndigheder, der skal føre tilsyn med direktivet på nationalt plan for de omfattede sektorer, jf. artikel 8, stk. 1 og 2. Da Finanstilsynet i dag er den kompetente myndighed på det finansielle område, vil det være Finanstilsynet, der skal føre tilsyn med NIS-direktivets overholdelse for så vidt angår det finansielle område.

Det følger endvidere af NIS-direktivets artikel 8, at hver medlemsstat udpeger et nationalt centralt kontaktpunkt for sikkerheden i net- og informationssystemer (centralt kontaktpunkt). Det nationale centrale kontaktpunkt udgør et forbindelsesled til at sikre grænseoverskridende samarbejde mellem medlemsstaternes myndigheder og de relevante myndigheder i andre medlemsstater samt den europæiske samarbejdsgruppe som nedsættes i medfør af direktivets artikel 11 og som skal bestå af repræsentanter fra medlemsstaterne, Kommissionen og Enisa, og det såkaldte CSIRT-netværk.

Det følger af direktivets artikel 12, at CSIRT-netværket oprettes for at bidrage til skabelsen af tillid mellem medlemsstaterne og at fremme et hurtigt og effektivt operationelt samarbejde. Netværket skal bestå af de nationalt udpegede CSIRTer (Computer Security Incident Response Team). En CSIRT's rolle vil som minimum omfatte monitorering af hændelser på nationalt plan, tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser, at reagere på hændelser, udarbejdelse af dynamisk risiko- og hændelsesanalyser og situationsrapporter.

Det følger endvidere af direktivets artikel 1, nr. 5, at oplysninger der er fortrolige i henhold til EU-regler og nationale regler, kan udveksles med forbehold af artikel 346 i TEUF, 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.

Dertil kommer, at det følger af præambel nr. 41 i NIS-direktivet, at hvis der er tale om oplysninger, der 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 direktivet.

3.2.3.3. Erhvervsministeriets overvejelser og den foreslåede ordning

NIS-direktivet indeholder en række krav om myndighedernes samarbejde på EU-niveau og på nationalt niveau og indeholder bl.a. i artikel 9 et krav om, at hver medlemsstat udpeger et nationalt centralt kontaktpunkt og en såkaldt CSIRT. I Danmark forventes Center for Cybersikkerhed, at blive udpeget som både nationalt centralt kontaktpunkt og som CSIRT.

Det nationale kontaktpunkt vil bl.a. i henhold til NIS-direktivet skulle orientere kontaktpunkter i andre medlemsstater om hændelser, der har væsentlige konsekvenser for kontinuiteten i de væsentlige tjenester, der udbydes i de pågældende lande.

Ifølge NIS-direktivet, skal en CSIRT som minimum monitorere hændelser på nationalt plan, modtage tidlige varslinger, advarsler og meddelelser om risici og hændelser og reagere på hændelser m.v.

Finanstilsynet er underlagt en skærpet tavshedspligt efter henholdsvis § 354 i lov om finansiel virksomhed og § 224 i lov om kapitalmarkeder, hvorefter Finanstilsynet er forpligtet til at hemmeligholde fortrolige oplysninger, som Finanstilsynet kommer i besiddelse af i medfør af tilsynsvirksomheden. I medfør af § 354, stk. 6, i lov om finansiel virksomhed og § 225 i lov om kapitalmarkeder, kan Finanstilsynet dog videregive en række oplysninger under nærmere fastsatte betingelser.

Henset til at det i øvrigt følger af NIS-direktivet, at oplysninger, der er fortrolige i henhold til EU-regler og nationale regler, kan udveksles, hvis en sådan udveksling er nødvendig for anvendelsen af dette direktiv, bør Finanstilsynets gives hjemmel til at videregive oplysninger om hændelser, som modtages fra operatørerne af væsentlige tjenester.

For at sikre det nationale samarbejde er det nødvendigt, at Finanstilsynet skal kunne udveksle oplysninger med Center for Cybersikkerhed.

Med lovforslaget foreslås det derfor at indføre mulighed for, at Finanstilsynet i medfør af henholdsvis lov om finansiel virksomhed og lov om kapitalmarkeder, kan videregive oplysninger til Center for Cybersikkerhed, under forudsætning af at oplysningerne er nødvendige for Center for Cybersikkerhed til opfyldelse af deres lovbestemte opgaver, i deres egenskab af nationalt centralt kontaktpunkt eller CSIRT.

Ligesom det gælder i dag ved Finanstilsynets videregivelse af fortrolige oplysninger, vil fortroligheden følge oplysningerne, hvilket indebærer, at for så vidt angår de oplysninger, som Finanstilsynet videregiver til Center for Cybersikkerhed, så indebærer videregivelsen, at Center for Cybersikkerhed omfattes af den samme skærpede tavshedspligt som Finanstilsynet er underlagt efter henholdsvis § 354 i lov om finansiel virksomhed og § 224 i lov om kapitalmarkeder. Dette er i øvrigt i overensstemmelse med NIS-direktivet, hvoraf det følger af præambel nr. 41, at hvis der er tale om oplysninger, der betragtes som værende fortrolige i overensstemmelse med EU-regler og nationale regler om forret-

ningshemmeligheder, bør denne fortrolighed sikres under udførelsen af aktiviteterne og opfyldelsen af målene i direktivet. Dertil kommer, at det følger af artikel 5, stk. 1, at oplysninger der er fortrolige i henhold til EU-regler og nationale regler, kan udveksles med forbehold af artikel 346 i TEUF, 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.

Endelig skal det bemærkes, at ved en eventuel videregivelse af personoplysninger vil de gældende regler vedrørende persondataloven tillige finde anvendelse, hvorfor behandling af persondata altid vil ske under iagttagelse af gældende lovgivning, herunder den kommende persondataforordning.

3.2.4. Offentliggørelse af hændelser

3.2.4.1. Gældende ret

Der er ikke i dag mulighed for, at Finanstilsynet kan offentliggøre konkrete oplysninger om hændelser.

Persondataloven regulerer behandling af personoplysninger, som foretages af offentlige myndigheder og private, når behandlingen helt eller delvist foretages ved hjælp af elektronisk databehandling. Den omfatter ligeledes ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, jf. § 1, stk. 1, i persondataloven. Persondatalovens regler gælder endvidere for anden ikke-elektronisk systematisk behandling af personoplysninger, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden, jf. § 1, stk. 2, i persondataloven. Af bemærkningerne til § 2, stk. 1, i persondataloven, jf. lov nr. 429 af 31. maj 2000 (lovforslag nr. L 147 af 9. december 1999), fremgår det, at bestemmelsen indebærer, at persondataloven finder anvendelse, hvis regler om behandling af personoplysninger i anden lovgivning giver den registrerede en dårligere retsstilling. Det fremgår imidlertid også, at dette ikke gælder, hvis den dårligere retsstilling har været tilsigtet og i øvrigt ikke strider mod 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 (databeskyttelsesdirektivet).

Det skal i den forbindelse bemærkes, at persondataloven gennemfører databeskyttelsesdirektivet, som ophæves pr. 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. forslagets § 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, der regulerer området for behandling af personoplysninger.

3.2.4.2. NIS-direktivet

Det fremgår af NIS-direktivets artikel 14, stk. 6, at den kompetente myndighed efter høring af den underrettende operatør af væsentlige tjenester kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

3.2.4.3. Erhvervsministeriets overvejelser og den foreslåede ordning

Finanstilsynet har ikke i dag mulighed for at offentliggøre konkrete oplysninger om hændelse, hvorfor en sådan bestemmelse bør indføres, både for så vidt angår lov om finansiel virksomhed og lov om kapitalmarkeder.

Med henblik på at sikre en direktivnær implementering foreslås det at indsætte en ny § 354 h i lov om finansiel virksomhed og en ny § 236 a i lov om kapitalmarkeder, hvorefter Finanstilsynet kan orientere offentligheden om konkrete hændelser, efter høring af den berørte virksomhed, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangværende hændelse. Offentliggørelsen må dog ikke indeholde fortrolige oplysninger om kundeforhold eller oplysninger omfattet af § 30 i lov om offentlighed i forvaltningen. Offentliggørelsen må ikke indeholde fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den Europæiske Union, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse.

Forslaget om offentliggørelse af oplysninger om hændelser, som ovenfor beskrevet, er udarbejdet med baggrund i de anbefalinger, som fremgår af Justitsministeriets betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser m.v. I betænkningen anbefales det, at der inden indførelse af ordninger med systematisk offentliggørelse af oplysning om kontrolresultater, afgørelser m.v. på internettet i ikke-anonymiseret form foretages en vurdering af det konkrete behov for offentliggørelse, om offentliggørelse kan forventes konkret at være særligt indgribende for personen, om der er tungtvejende samfundsmæssige hensyn bag offentliggørelsesordningen, om offentliggørelse strider mod persondataloven og de almindelige regler om tavshedspligt, og om der af retssikkerhedsmæssige grun-

de er opstillet administrative regler for forvaltningsmyndighedens behandling af de enkelte sager.

Det vil således være Finanstilsynets vurdering, om det er nødvendigt for at forebygge eller håndtere en igangværende hændelse at offentliggøre navnet på den berørte virksomhed, eller om det samme resultat kan nås med en anonymiseret offentliggørelse, som alene omfatter den konkrete hændelse. En offentliggørelse vil dog altid forudsætte, at den berørte virksomhed er blevet hørt herom.

4. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget medfører, at Erhvervsstyrelsen skal varetage nye opgaver. Disse opgaver forudsættes imidlertid afholdt inden for den eksisterende økonomiske ramme. Lovforslaget vurderes på den baggrund ikke at have økonomiske eller administrative konsekvenser for det offentlige.

I det omfang stat, kommuner og regioner er operatører af væsentlige tjenester eller udbyder digitale tjenester, vil de krav, der efter lovforslaget stilles til operatører og udbydere, også omfatte stat, kommuner og regioner. Det vil kunne medføre økonomiske og administrative konsekvenser i samme omfang som for private udbydere.

Lovforslaget medfører endvidere, at Finanstilsynet skal varetage nye opgaver, i form af udpegninger af operatører af væsentlige tjenester. Lovforslaget vurderes dog ikke i sig selv at have økonomiske eller administrative konsekvenser for det offentlige. Finanstilsynet vil derudover også skulle etablere et samarbejde med Center for Cybersikkerhed for så vidt angår håndtering og indberetninger af hændelser. Dette kan medføre behov for øgede ressourcer, men det er dog ikke muligt at kvantificere yderligere på nuværende tidspunkt.

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

Lovforslaget medfører økonomiske konsekvenser for operatører af væsentlige tjenester og udbydere af digitale tjenester.

Det vurderes, at lovforslaget medfører administrative konsekvenser under 4 mio. kr. årligt. Vurderingen bygger blandt andet på det relativt begrænsede antal hændelser årligt, der skal indberettes.

I forhold til de øvrige efterlevelseskonsekvenser vurderes disse at være under bagatelgrænsen på 10 millioner kroner årligt. Byrderne vil kunne angå omkostninger til fx it-udstyr og lønomkostninger til medarbejdere, der skal stå få opfyldelse af kravene. For en stor dels vedkommende vil dette være omkostninger, som operatørerne og udbyderne måtte forventes at have i forvejen.

I medfør af lovforslaget bemyndiges Finanstilsynet endvidere til at kunne fastsætte nærmere regler om indberetning af hændelser for operatører af væsentlige tjenester. Disse regler vil blive fastsat på bekendtgørelsesniveau og kan medføre økonomiske konsekvenser for de pengeinstitutter, realkreditinstitutter, operatører af markedspladser og centrale modparter (CCP'ere), der udpeges som operatører af væsentlige tjenester.

Det vurderes, at lovforslaget medfører minimale øvrige efterlevelsesomkostninger for erhvervslivet, under bagatelgrænsen på 10 millioner kroner årligt. Vurderingen bygger blandt andet på det relativt begrænsede antal hændelser årligt, der vil blive stillet specifikke krav til indberetningen af. Dette vil imidlertid blive kvantificeret i forbindelse med udarbejdelsen af eventuelle nye regler.

De administrative konsekvenser ved forslaget er blevet vurderet af Erhvervsstyrelsens Team Effektiv Regulering (TER), der vurderer, at forslaget ikke i sig selv medfører administrative konsekvenser på mere end 4 mio. kr. årligt. Konsekvenserne bliver derfor ikke kvantificeret nærmere.

6. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

8. 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, EU-Tidende 2016, nr. L 194, side 1. NIS-direktivet indebærer en minimumsharmonisering over for operatører af væsentlig tjenester, hvorimod direktivet er udtryk for totalharmonisering over for udbydere af digitale tjenester.

9. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den 17. oktober 2017 til den 17. november 2017 været sendt i høring hos følgende myndigheder og organisationer m.v.:

24-7 Net, 3Shape A/S, Abakomp Internet Service ApS, AciaNet, ACN, Activewebs A/S, Adapt Group A/S, Adform A/S, Advice Digital ApS, Advokatrådet, AF-Vejen, AirNet, Akademisk Arkitektforening, ALCO Company ApS, Altibox Danmark A/S, Andelskassen, Andelsnet ApS, Antenneforening Vejen, Antennelauget Flimmer, Arbejderbevægelsens Erhvervsråd, Arbejdsmarkedets Erhvervssygdomssikring (AES), Arbejdsmarkedets Tillægspension (ATP), Arbejdsskadestyrelsen, Ascio Technologies Inc. Danmark, Asiainfo Denmark ApS, Atea A/S, Athena IT-Group A/S, ATZtel, Aura Energi, Axcess A/S, Azehosting ApS, Balle-Bredsten Antenneforening, Banedanmark, Barablu, BC Hospitality Group A/S, Bjerringbro Kabelnet, Bluegarden A/S, Bo Data ApS, Bolignetforeningen, Bolignet-Aarhus, Boligselskabernes Landsforening, Bonavent Invest A/S, Bording Data A/S, Bornfiber, Boxer, Brancheforum Digitale Medier (Branchen ForbrugerElektronik), Bredalsparken, Bredbånd Nord, Bricksite ApS, Bruun Rasmussen Kunstauktioner A/S, Børsmæglerforeningen, Baagøe ApS, C & B Systemer

A/S, Cbrain A/S, CBS, CCI Europe A/S, Team Effektiv Regulering (TER), Cicoor Host & Saas ApS, Cirque Bredbånd A/S, Cloudnordic ApS, Co3 A/S, Colt Technology Services A/S, Columbus A/S, Combine, Comflex Networks ApS, Comm2ig A/S, Compusoft A/S, Concept Data A/S, Configit A/S, Connect-me, Conscia A/S, Corporate Services A/S, Cortex Consult A/S, CSC Danmark A/S, CSC Scandihealth A/S, Danaweb A/S, Dancenter A/S, DanDial Networks A/S, Dandomain A/S, Danhost ApS, Danish Venture Capital and Private Equity Association, Danmarks Grundforskningsfond, Danmarks Nationalbank, Danmarks Rederiforening, Danmarks Skibskredit A/S, Dansk Aktionærforening, Dansk Arbejdsgiverforening, Dansk Beredskabskommunikation A/S, Dansk BiblioteksCenter A/S, Dansk Byggeri, Dansk Ejendomsmæglerforening, Dansk Energi, Dansk Erhverv, Dansk Forening for International Motorkøretøjsforsikring (DFIM), Dansk Industri, Dansk Investor Relations Forening – DIRF, Dansk IT, Dansk Kabel TV A/S, Dansk Kredit Råd, Dansk Media, Dansk Metal, Dansk Pantebrevsforening, Danske Advokater, Danske eWire A/S, Danske Forsikringsfunktionærers Landsforening, Danske Handicaporganisationer, Danske Maritime, Danske Medier, Danske Regioner, DanskNet A/S, Datagruppen Multimed A/S, Den Danske Aktuarforening, Den Danske Dommerforening, Den Danske Finansanalytikerforening, Den danske Fondsmæglerforening, Det Centrale Handicapråd, Dialoga Group, Dansk Internet Forum (DIFO), DI Digital, Digital Rights, Digizuite A/S, Dis/Play A/S, DK-Hostmaster A/S, DLG Tele, DLX A/S, Dyrup Sanderum Antenneforening, EbeltoftS.net, Economic International A/S, Edlund A/S, Eg A/S, Ejendomsforeningen, Elro Erhverv A/S, Ementor Danmark A/S, Energi Fyn, Energi og Olieforum, EnergiMidt, Entertainment Trading ApS (Coolshop), Eriksminde Medienet, Evercall ApS, EWII, Exaweb ApS, Facilicom A/S, Falcon.io ApS, FasCom A/S, Fastline, FDA, FDE, FDFA – Foreningen af Danske Forsikringsmæglere og Forsikrings Agenturer, FDIH – Foreningen for Distance- og Internethandel, Fest.Dk A/S, Fiber2you, Fiberby, Fibia, Finans og Leasing, Finans-Danmark, Finansforbundet, Finanshuset i Fredensborg A/S, Finansiel Stabilitet, Finansrådet, Finanssektorens Arbejdsgiverforening, Fionia IT ApS, Firstcom A/S, Fonet A/S, Forbrugerombudsmanden, Forbrugerrådet, Forbrugsforeningen, Foreningen af Danske Internet Medier (FDIM), Foreningen af Forretningsførere for Udenlandske Forsikringsselskaber, Foreningen af Interne Revisorer, Foreningen Bankdata, Foreningen Danske Revisorer, FOREX, Forsikring & Pension, Forsikringens Datacenter A/S, Forsikringsmæglerforeningen, Frivilligrådet, Fsa-net.dk, FSR – danske revisorer, Funktionærernes og Tjenestemændenes Fællesråd (FTF), Faaborg Vest Antenneforening, FaaborgVestAF, G4S Security Services A/S, Galten Elværk, Garantiformuen, Garban-Intercapital Scandinavia, GE Erhverv A/S, GEV A/S, Gigabit, Gigahost ApS, Glenten, Global Crossing, GlobalConnect A/S, GlobalTel, Golden Planet ApS, Gram Bynet, GVD, Gørlev Antenneforening, Hansen Technologies Denmark A/S, HAS Hjørring Antenneselskab, HashøjNet, HEF, Hi3G Denmark ApS, Hiper, Horesta, Hosters A/S, Hosthouse Avalonia ApS, Hostnordic A/S, Højen Antennelaug, Høng Antennelaug, Håndværksrådet, Hårlev Antenneforening, I P Group A/S, I/S Bredbånd Nord, IBM Danmark, ICE. NET/Net1, Indsamlingsorganisationernes Brancheorganisation (ISOBRO), Info Key A/S, Info-Connect A/S, Infolink ApS, Installa'sjon, Internet Danmark Holding ApS, Internet4u/Computer Problemer, Intertrust (Denmark), Inventio.it A/S, Investeringsfondsbranchen, IP Group, ipnordic A/S, Ipvision A/S, ISACA Denmark Chapter, IT Forum Gruppen A/S, IT Overblik ApS, It Relation A/S, IT Universitetet, IT-Afdelingen A/S, IT-Branchen, Itide A/S, It-Kompagniet Jylland ApS, IT-Lauget Parknet, Itpilot ApS, IT-Politisk Forening, IT-R ApS, ITR Data A/S, J. H. Schultz Information A/S, Jansson Kommunikation A/S, Jaynet A/S, JCD A/S, Jels Antenneforening, Jerlev Antenneforening, JN Data A/S, Just Eat.dk ApS, Kabelplus, Kalundborg AF, Kjærgaard A/S, Kjærgaard-Nettet, Klarup Kabelnet, Klein-Data, KMD A/S, KommuneKredit, Kommunernes Landsforening, Konform A/S, Kortermann-Hosting ApS, Korup Antennelaug, Kronholm Kommunikation, Kuratorforeningen, Kviknet, Københavns Energi, Købmandstandens OplysningsBureau, Landbrug & Fødevarer, Landsforeningen af forsvarsadvokater, Landsforeningen for Bæredygtigt Landbrug, Landsorganisationen i Danmark (LO), Larsen Data ApS, Lauritz.com A/S, Lebera Mobile Danmark, LEGO GROUP, Lessor A/S, Lokale Pengeinstitutter, Lollands.net, Lycamobile, Lønmodtagernes Dyrtidsfond (LD), Markmonitor ApS, Maxtel.dk ApS, Mb Solutions A/S, Mediaconnect ApS, Mentor It A/S, Mira Internet ApS, Miracle A/S, Montes A/S, Morud Antenneforening, Mundio Mobile ApS, MWAzone, Mybanker, NAL MedieNet ApS, NASDAQ Copenhagen A/S, NEF Fiber A/S, Netcompany A/S, Net-group A/S, Netic A/S, Netip A/S, netordre.dk ApS, Netplan System Design.dk ApS, Nets Denmark A/S, Netsite A/S, Netteam A/S, NetTel ApS, Newangle Software ApS, Newwweb ApS, Next Level Internet A/S, NHC A/S, NHL Data ApS, Nianet A/S, NM Net ApS, Nn Hosting, NNIT A/S, Nordby Antenneforening/Fanø Net, Nordby AF, Nordea, Nordic Connect, Nordit A/S, Novasol A/S, Novicell ApS, NRGi, NTI Cadcenter A/S, Nyfors, Odder Antenneforening, One.com A/S, Orange Business Services Denmark A/S, Origo Systems ApS, Osted Nettet, Parcelhusejernes Landsforening, Parknet, PDC A/S, Pentacon A/S, Perspektiv Bredbånd, Phone-IT A/S, PIL - Professionelle Internet Løsninger ApS, Pi-Web I/S, Plenti, PLM Group ApS, plusTEL ApS, PMR-brugergruppen, Polperro A/S, PostNord, Powerhosting ApS, Powernet ApS, Primanet, Proactive A/S, ProData Consult A/S, PROSA - Forbundet af it-professionelle, Proudwing ApS, Præstø Antennelaug, Puzzel A/S, Rambøll Danmark A/S, Redspot ApS, Region Hovedstaden, Regionale Bankers Forening, Revisornævnet, Ricoh Danmark A/S, Rosenholms Net, Rådet for større IT-sikkerhed, Sac-IT A/S, Sagitta ApS, Sammenslutning af Lokale Radio- og TV-stationer, Samsø Bredbånd, Saxo Payments A/S, Schantz A/S, SE Fibernet A/S, SEAS-NVE, SEF Fiber, Semler Services A/S, Service Center Fyn/ Lars Falck Jershauge, Shopstart ApS, Silkeborg Data A/S, SimCorp A/S, Sitecore Cor-

poration A/S, Skagen Antennelaug, Skagennet, Skibs- og Bådebyggeriets Arbejdsgiverforening, Skjern Bredbånd, Skodborg Antennelaug, Skovsby Internet, Softwork ApS, Sol og Strand Feriehusudlejning A/S, Solutio ApS, Sprint-Link Danmark ApS, Stilmark, Stofa A/S, Sundbynet, Syd Energi, Syddansk Universitet, Sydfyns Intranet A/S, Systematic A/S, Systemhosting A/S, Sæby Antenneforening, Sønderho Antenneforening, Talk IP, TDC A/S, Team Nethosting ApS, Telanco ApS, Teleankenævnet, Telecom X ApS, Teleklagenævnet, Telekommunikationsindustrien i Danmark, Telenor A/S, Telia Danmark, Tellio ApS, Tetra-Star A/S, ThomsenTrampedach, Thomson Reuters Nordic, Thyfon A/S, Thy-Mors Energi A/S, Tia Technology A/S, Timecomputer A/S, Tjeep, Toftlund Bynet, Transparency International Danmark, Travelmarket A/S, TREFOR Bredbånd A/S, Trifork A/S, Truecommerce Denmark ApS, Trådløsfiber.dk, TS Computer ApS, Tune Kabelnet, UNI-C, Unik System Design A/S, Uni-tel A/S, Universal Telecom, Unwire, Uptime-IT ApS, Verdo Tele A/S, Verizon Business A/S, Vest Net A/S, VestjyllandS.net, Vestnet ApS, Videbæk Antenneforening, Vindinge Antennelaug, Viptel ApS, Visma Consulting A/S, VK Data ApS, VP Securities A/S, Waoo! A/S, Webbureauet Infoserv ApS, Webhosting A/S, Webhot ApS, Western Union, Wified, WWI A/S, Yaygroup I/S, Yderholm Antenneforening, ZebNet, ZenSystem, Zibra Wireless, Zitcom A/S, Ønet, Ørum Net, Aalborg Universitet, Aalbæk Bugt Antenneforening, Årslev Net, Færøernes Hjemmestyre via Rigsombudsmanden på Færøerne, Grønlands Selvstyre via Rigsombudsmanden i Grønland, Beskæftigelsesministeriet, Børne- og Socialministeriet, Energi-, Forsynings- og Klimaministeriet, Erhvervsministeriet, Finansministeriet, Forsvarsministeriet, Justitsministeriet, Kirkeministeriet, Kulturministeriet, Miljø- og Fødevareministeriet, Skatteministeriet, Statsministeriet, Sundheds- og Ældreministeriet, Transport-, Bygnings- og Boligministeriet, Uddannelses- og Forskningsministeriet, Udenrigsministeriet, Udlændinge- og Integrationsministeriet, Undervisningsministeriet, Økonomi- og Indenrigsministeriet, Arbejdsskadestyrelsen, Beredskabsstyrelsen, Datatilsynet, Energistyrelsen, Forsvarets Efterretningstjeneste, Konkurrence- og Forbrugerstyrelsen, Moderniseringsstyrelsen, Patent- og Varemærkestyrelsen, Politiets Efterretningstjeneste, Rigspolitiet, Rigsrevisionen, Sikkerhedsstyrelsen, Statens It, Statsadvokaten for Særlig Økonomisk og International Kriminalitet, Styrelsen for It og Læring, Søfartsstyrelsen, Nævnenes Hus, Udbetaling Danmark.

10. Sammenfattende skema

Samlet vurdering af konsekvenser af lovforslaget

	Positive konsekvenser/ mindreudgifter (hvis ja, angiv omfang)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner, og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Det vurderes, at lovforslaget i forhold til de øvrige efterlevelseskonsekvenser medfører byrder under bagatelgrænsen på 10 millioner kroner årligt.
Administrative konsekvenser for erhvervslivet	Ingen	Det vurderes, at lovforslaget medfører administrative byrder under 4 mio. kr. årligt.
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, EU-Tidende 2016, nr. L 194, side 1.	
Overimplementering af EU-retlige minimumsforpligtelser (sæt X)	JA	NEJ X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Den foreslåede bestemmelse i § 1 beskriver anvendelsesområdet for loven.

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

Efter *§ 1, stk. 1*, finder lovforslaget anvendelse på operatører af væsentlige tjenester inden for den digitale infrastruktur og udbydere af digitale tjenester, jf. dog stk. 2.

Operatører af væsentlige tjenester er væsentlige domænenavnssystemer og topdomænenavneadministratorer, der er etableret i Danmark. Med etableret menes en effektiv og reel udøvelse af aktiviteter gennem stabile ordninger. Den retlige form er ikke afgørende og kan ud over operatører med hjemsted i Danmark også omfatte ordninger med status som juridisk person i form af fx filialer og datterselskaber.

Udbydere af digitale tjenester er udbydere af onlinemarkedspladser, onlinesøgemaskiner eller cloud computing-tjenester, der enten har hovedsæde i Danmark eller har en repræsentant i landet. Udbydere af digitale tjenester, der tilbyder deres tjenester i Danmark, men som ikke har hovedsæde i landet eller en anden EU-medlemsstat, vil skulle udpege en repræsentant, jf. lovforslagets § 7.

Lovforslagets § 1, stk. 1, gennemfører på denne baggrund NIS-direktivets bestemmelser om operatører af væsentlige tjenester inden for den digitale infrastruktur og udbydere af digitale tjenester i Danmark på Erhvervsministeriets område.

Efter den foreslåede *stk. 2*, finder loven ikke anvendelse på udbydere af digitale tjenester i form af mikrovirksomheder eller små virksomheder. Bestemmelsen gennemfører artikel 16, stk. 11, i NIS-direktivet, hvorefter mikrovirksomheder og små virksomheder ikke er omfattet af kravene til udbydere af digitale tjenester. Mikrovirksomheder og små virksomheder skal forstås i overensstemmelse med definitionen i Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder. Det vil således være udbydere af digitale tjenester med mindst 50 ansatte og en årlig omsætning eller en årlig balance over 10 mio. EUR, der vil være omfattet af kravene. Denne undtagelse skal ses i sammenhæng med, at det skal undgås, at udbydere pålægges en uforholdsmæssig stor finansiel og administrativ byrde, og at kravene til udbyderne skal stå i rimeligt forhold til den konkrete risiko.

Til § 2

Den foreslåede § 2 definerer 18 centrale begreber i loven. Definitionerne i nr. 1, 2 og 4-15 er indholdsmæssig identiske med de tilsvarende definitioner i NIS-direktivet.

Efter *nr. 1* er definitionen af net- og informationssystem indholdsmæssigt identisk med definitionen af net- og informationssystem i NIS-direktivets artikel 4, nr. 1. Definitionen af elektroniske kommunikationsnet er enslydende med den definition af elektroniske kommunikationsnet, der anvendes i lov om elektroniske kommunikationsnet og -tjenester. Sidstnævnte lov implementerer Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), som definitionen i NIS-direktivet artikel 4, nr. 1, er baseret på.

Efter *nr. 2* er definitionen af sikkerhed i net- og informationssystemer indholdsmæssigt identisk med definitionen af sikkerhed i net- og informationssystemer i NIS-direktivets artikel 4, nr. 2.

Efter *nr. 3* foreslås definitionen af operatør af tjenester at omfatte alle offentlige eller private enheder i Danmark, som leverer en DNS-tjeneste eller er administrator af et topdomænenavn, uanset om enhedens aktiviteter opfylder kriterierne i § 3.

Efter *nr. 4* er definitionen af operatør af væsentlige tjenester indholdsmæssigt identisk med definitionen operatør af væsentlige tjenester i NIS-direktivets artikel 4, nr. 4.

Efter *nr. 5* er definitionen af digital tjeneste indholdsmæssigt identisk med definitionen af digital tjeneste i NIS-direktivets artikel 4, nr. 5.

Efter *nr. 6* er definitionen af udbyder af digitale tjenester indholdsmæssigt identisk med definitionen af udbyder af digitale tjenester i NIS-direktivets artikel 4, nr. 6.

Efter *nr. 7* er definitionen af hændelse indholdsmæssigt identisk med definitionen af hændelse i NIS-direktivets artikel 4, nr. 7.

Efter *nr. 8* er definitionen af risiko indholdsmæssigt identisk med definitionen af risiko i artikel 4, nr. 9.

Efter *nr. 9* er definitionen af repræsentant indholdsmæssigt identisk med definitionen af repræsentant i NIS-direktivets artikel 4, nr. 10.

Efter *nr. 10* er definitionen af domænenavnesystem (DNS) indholdsmæssigt identisk med definitionen af domænenavnesystem (DNS) i NIS-direktivets artikel 4, nr. 14.

Efter *nr. 11* er definitionen af DNS-tjenesteudbyder indholdsmæssigt identisk med definitionen af DNS-tjenesteudbyder i NIS-direktivets artikel 4, nr. 15.

Efter *nr. 12* er definitionen af topdomænenavneadministrator indholdsmæssigt identisk med definitionen af topdomænenavneadministrator i NIS-direktivets artikel 4, nr. 16.

Efter *nr. 13* er definitionen af onlinemarkedsplads indholdsmæssigt identisk med definitionen af onlinemarkedsplads i NIS-direktivets artikel 4, nr. 17. Af NIS-direktivets betragtning 15 fremgår det yderligere, at onlinemarkedsplads ikke omfatter onlinetjenester, der kun tjener til at formidle tredjepartstjenester, hvor en kontrakt kan indgås i sidste ende. Definitionen af onlinemarkedsplads omfatter heller ikke 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.

Efter *nr. 14* er definitionen af onlinesøgemaskine indholdsmæssigt identisk med definitionen af onlinesøgemaskine i NIS-direktivets artikel 4, nr. 18. Af NIS-direktivets betragtning 16 fremgår det yderligere, at definitionen af onlinesøgemaskine ikke omfatter søgefunktioner, der er begrænset til indholdet af et særligt websted, uanset om søgefunktionen er fra en ekstern søgemaskine. Den omfatter heller ikke onlinetjenester, der sammenligner prisen på bestemte varer eller tjenester fra forskellige erhvervsdrivende og derefter omdirigerer brugeren til den foretrukne erhvervsdrivende for at købe produktet.

Efter *nr. 15* er definitionen af cloud computing-tjeneste indholdsmæssigt identisk med definitionen af cloud computing-tjeneste i NIS-direktivets artikel 4, nr. 19. Af NIS-direktivets betragtning 17 fremgår det yderligere, at it-ressourcer omfatter ressourcer som fx 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 udstyr.

Efter *nr. 16* bygger definitionen af nationalt centralt kontaktpunkt på beskrivelsen heraf i NIS-direktivets artikel 8.

Efter *nr. 17* bygger definitionen af CSIRT på beskrivelsen heraf i NIS-direktivets artikel 9 og bilag 1.

Efter *nr. 18* er definitionen af mikrovirksomheder og små virksomheder identisk med den tilsvarende definition af mikrovirksomheder og små virksomheder i Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder. Virksomheder med 49 eller færre ansatte og en årlig omsætning eller en årlig balance på 10 mio. EUR eller mindre betragtes som værende mikrovirksomheder og små virksomheder.

Til § 3

Den foreslåede § 3 i lovforslaget gennemfører artikel 5 i NIS-direktivet.

Efter den foreslåede *§ 3, stk. 1*, skal en enhed anses for en operatør af en væsentlig tjeneste, hvis 1) enheden leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, 2) leveringen af tjenesten afhænger af net- og informationssystemer, og 3) en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste. Med stk. 1, fastlægges de overordnede kriterier for, hvornår en offentlig eller privat enhed, der udbyder en tjeneste inden for administration af domænenavne- eller topdomænenavnesystemer, skal betragtes som en operatør af en væsentlig tjeneste.

I afklaringen af om en tjeneste er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter vil den ansvarlige for en enhed skulle tage udgangspunkt i den liste over væsentlige tjenester, som erhvervsministeren udarbejder i henhold til lovforslagets § 3, stk. 2. I vurderingen skal derudover indgå, om tjenesten er afhængig af net- og informationssystemer, og om en hændelse vil få væsentlig forstyrrende virkning for leveringen af den pågældende tjeneste. For domænenavnssystemer og digitale tjenester vil betingelsen om, at disse er afhængig af net- og informationssystemer, altid være opfyldt, idet det er en integreret del af de pågældende systemer og tjenester. Net- og informationssystemer skal forstås i overensstemmelse med definitionen i lovforslagets § 2, nr. 1.

I vurderingen af, hvorvidt en hændelse vil få væsentlig forstyrrende virkning, vil en række faktorer skulle indgå, som fx det antal brugere, der er afhængige af tjenesten til private eller erhvervsmæssige formål. Brugen af tjenesten kan her være 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, vil ligeledes kunne indgå, hvor lang tid der skønnes at ville gå, før afbrydelsen af tjenesten vil have negative konsekvenser. Kriterierne for, hvornår en hændelse har væsentligt forstyrrende virkning, vil blive nærmere fastsat af erhvervsministeren i henhold til bemyndigelsesbestemmelsen i lovforslagets § 5, stk. 4.

Efter lovforslagets *§ 3, stk. 2*, udarbejder og opdaterer erhvervsministeren en liste over væsentlige tjenester. Med bestemmelsen får erhvervsministeren bemyndigelse til at udarbejde og regelmæssigt ajourføre en liste over tjenester inden for den digitale infrastruktur, der er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter. Listens formål er at identificere de typer af væsentlige tjenester, der findes inden for administration af domænenavnesystemer eller topdomænenavnesystemer. Dette betyder, at den ansvarlige enhed inden for denne sektor kan holde de væsentlige tjenester adskilt fra de ikke-væsentlige aktiviteter. Den nærmere afgrænsning af væsentlige tjenester vil tage udgangspunkt i tjenester, der er vigtige for samfundets funktionalitet, og hvor en afbrydelse fx vil hindre gennemførelsen af økonomiske aktiviteter, underminere brugernes tillid og på anden måde gøre skade på samfundsøkonomien.

Efter lovforslagets *§ 3, stk. 3*, kan erhvervsministeren fastsætte nærmere regler for afgrænsningen af operatører af væsentlige tjenester. Det er hensigten at få fastlagt grænseværdier, fx i form af brugen af en væsentlig tjeneste, der afgrænser, hvornår en operatør anses for at være drive en væsentlig tjeneste.

Til § 4

Den foreslåede § 4 i lovforslaget gennemfører dele af artikel 14 i NIS-direktivet. Med lovforslaget fastlægges sikkerhedskravene for operatører af væsentlige tjenester.

Efter det foreslåede *§ 4, stk. 1*, skal operatører af væsentlige tjenester træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i de 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 mål med risikoen. Bestemmelsen gennemfører artikel 14, stk. 1, i NIS-direktivet.

Efter lovforslagets *§ 4, stk. 2*, skal operatører af væsentlige tjenester endvidere træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer, som anvendes til levering af væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester. Bestemmelsen gennemfører NIS-direktivets artikel 14, stk. 2.

Bestemmelserne i lovforslagets § 4, stk. 1 og 2, skal ses i sammenhæng. Formålet med begge bestemmelser er således at fremme en risikostyringskultur med risikovurdering og gennemførelse af sikkerhedsforanstaltninger, som står i forhold til risiciene. Det er her afgørende, at operatørerne ikke pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, hvorfor kravene skal stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende net- og informationssystem, under hensyntagen til sådanne foranstaltningers aktuelle stade.

Bestemmelserne i lovforslagets § 4, stk. 1 og 2, vil indebære, at operatørerne skal arbejde systematisk og risikobaseret med sikkerheden i deres net- og informationssystemer. Risikostyringsforanstaltningerne vil omfatte 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 og skal ses som evnen til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i systemerne.

I tilfælde, hvor der er tale om behandling af personhenførbare oplysninger, vil lovgivningen for databeskyttelse, jf. Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger, finde tilsvarende anvendelse. Reglerne i databeskyttelsesforordningen vil finde anvendelse, når disse træder i kraft den 25. maj 2018.

Foranstaltningerne skal tage højde for den teknologiske udvikling. Operatørerne vil i forlængelse heraf i deres tilrettelæggelse og ajourføring af deres sikkerhedsforanstaltninger skulle inddrage de tekniske løsninger, der er tilgængelige på markedet.

Med tekniske foranstaltninger sigtes her til foranstaltninger, der er med til at sikre it-sikkerheden (datasikkerhed og kommunikationssikkerhed) og den fysiske sikkerhed. Tekniske foranstaltninger vil i forlængelse heraf fx være foranstaltninger, der skal beskytte enten net- og informationssystemerne og operatørernes fysiske lokaliteter mod uberettiget adgang for udefrakommende, eller sikre at data kan overføres sikkert. Organisatoriske foranstaltninger sigter til fx styredokumenter, manualer, monitorering og evaluering af sikkerhedsindsatsen.

Hvilke foranstaltninger inden for lovgivningens rammer, der konkret skal træffes, overlades til operatørerne. Bestemmelsen indfører ikke en forpligtelse til at konstruere, udvikle eller fremstille et bestemt kommercielt informations- og kommunikationsteknologiprodukt. Sikkerhedskravene gælder endelig uanset om operatørerne selv står for vedligeholdelsen af deres net- og informationssystemer eller har outsourcet denne opgave.

Efter lovforslagets *§ 4, stk. 3*, kan erhvervsministern fastsætte nærmere regler om foranstaltninger efter stk. 1 og 2. Med bestemmelsen vil erhvervsministeren få bemyndigelse til at fastsætte nærmere sikkerhedskrav til operatørerne. Bemyndigelsen vil skulle anvendes til at præcisere lovforslagets krav i § 4, stk. 1 og 2, om risikostyringsforanstaltninger på baggrund af bl.a. de vejledninger, der ventes udstedt i EU-regi om operatørernes sikkerhedsforpligtelser i henhold til NIS-direktivet. Bemyndigelsen kan fx anvendes til at fastsætte bestemmelser om adgang, til fysisk- og miljømæssig sikkerhed såsom beskyttelse mod indbrud og brand, samt bestemmelser om forsyningssikkerhed såsom udarbejdelse af politikker for adgang til elforsyning.

Bemyndigelsen vil ikke blive anvendt til at fastsætte yderligere krav end de krav, der følger af NIS-direktivet. Endvidere vil der i udmøntningen af bemyndigelsen blive lagt vægt på at sikre, at operatørerne kun underlægges proportionale krav, der i videst muligt omfang overlader et skøn til udbyderne til selv at beslutte indholdet af deres sikkerhedsforanstaltninger, så længe de er tilstrækkelige til at leve op til sikkerhedsforpligtelserne.

Til § 5

Den foreslåede § 5 i lovforslaget gennemfører dele af artikel 14 i NIS-direktivet. Med lovforslaget fastlægges operatørers forpligtelse til at underrette myndighederne i tilfælde af hændelser.

Efter lovforslagets *§ 5, stk. 1*, skal operatører af væsentlige tjenester hurtigst muligt underrette Erhvervsstyrelsen 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 Erhvervsstyrelsen og Center for Cybersikkerhed at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. Med bestemmelsen vil underretningen skulle indeholde oplysninger, der gør Erhvervsstyrelsen og Center for Cybersikkerhed i stand til at vurdere om hændelsen har betydning for andre EU-lande, fx antal brugere af de berørte systemer i de pågældende lande og varigheden af hændelsen.

Hændelser defineres her i overensstemmelse med lovforslagets § 2, nr. 7, hvorefter en hændelse er enhver begiven-

hed, der har egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.

Med hurtigst muligt sigtes til, at operatøren under hensyntagen til arbejdet med at minimere konsekvenserne af hændelsen skal foretage underretningen, så snart denne har de nødvendige oplysninger til at kunne vurdere omfanget af hændelsen. Det gælder særligt, hvis hændelsen vurderes at kunne påvirke flere operatører eller til at være grænseoverskridende, hvilket fx kan være tilfældet ved en hændelse, som rammer et topdomænenavn.

Efter det foreslåede *stk. 2* skal operatøren i vurderingen af, om en hændelse har væsentlige konsekvenser navnlig inddrage: a) antallet af brugere, der er berørt af hændelsen, b) hændelsens varighed og c) hvor stort et geografisk område, der er berørt af hændelsen. De nærmere kriterier for, hvornår og hvordan en underretning vil skulle ske samt indholdet af underretningen, vil blive fastlagt af erhvervsministeren i henhold til bemyndigelsesbestemmelsen i lovforslagets § 5, stk. 4. Bliver Erhvervsstyrelsen bekendt med, at der ikke er foretaget underretning af en hændelse, som har væsentlige konsekvenser, vil der som udgangspunkt blive udstedt et påbud om at foretage underretningen. Manglende opfyldelse af påbuddet er straffebelagt, jf. lovforslagets § 17.

Efter det foreslåede *stk. 3* skal operatøren også foretage en underretning, hvis dennes net- og informationssystemer er påvirkede af en hændelse i en digital udbyders tjeneste, som operatøren er afhængig af. Herigennem sikres, at Erhvervsstyrelsen og Center for Cybersikkerhed får kendskab til hændelser og mangler i sikkerheden hos udbydere af digitale tjenester, der har en negativ indvirkning på væsentlige tjenester. Underretningen vil kunne indgå som dokumentation for, at en udbyder ikke har levet op til kravene efter dette lovforslag. Bestemmelsen i stk. 3 er indholdsmæssig identisk med artikel 16, stk. 5, i NIS-direktivet.

Efter det foreslåede *stk. 4* kan erhvervsministeren fastsætte nærmere regler om underretning efter stk. 1 og 3, og om kriterierne efter stk. 2. Det er hensigten at få fastlagt grænseværdier for, hvornår en hændelse anses for væsentlig. Det forventes, at indberetning vil skulle ske via en fælles indberetningsløsning, fx på virk.dk.

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 unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet, jf. persondataforordningens art. 33, stk. 1.

Til § 6

Den foreslåede § 6 i lovforslaget gennemfører dele af artikel 14 i NIS-direktivet.

Med bestemmelsen i *stk. 1* foreslås det, at Erhvervsstyrelsen kan videregive oplysninger til Center for Cybersikkerhed om hændelser, der er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver som nationalt centralt kontaktpunkt og CSIRT i henhold til NIS-direktivet. Bestemmelsen skal anvendes i overensstemmelse med forvaltningslovens § 28 og under iagttagelse af de grundlæggende principper om saglighed og proportionalitet. 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. Center for Cybersikkerhed skal i henhold til direktivet foretage monitorering af hændelser på nationalt plan, tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser, at reagere på hændelser, udarbejdelse af dynamisk risiko- og hændelsesanalyser og situationsrapporter. Center for Cybersikkerhed vil endvidere skulle orientere kontaktpunkter i andre medlemsstater om hændelser, der har væsentlige konsekvenser for kontinuiteten i de væsentlige tjenester, der udbydes i de pågældende lande - fx hændelser i forhold til tilgængeligheden af domænenavnsservertjenesten hos en væsentlig topdomænenavnsadministrator. Orienteringen vil ske under hensyntagen til operatørens sikkerhed og kommercielle interesser samt krav på fortrolig behandling af oplysninger.

Efter det foreslåede *stk. 2*, kan Erhvervsstyrelsen videregive relevante oplysninger til den underrettende operatør af væsentlige tjenester om opfølgningen på underretningen, herunder oplysninger der kan støtte en effektiv håndtering af hændelsen. Formålet med bestemmelsen er først og fremmest at sikre, at operatøren får en tilbagemelding, der kan understøtte operatørens videre arbejde med at begrænse hændelsen.

Med bestemmelsen i *stk. 3* foreslås det, at Erhvervsstyrelsen efter høring af den underrettende operatør af væsentlige tjenester oplyser offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse. Erhvervsstyrelsens beslutning om at offentliggøre en konkret hændelse er ikke en afgørelse i forvaltningslovens forstand. Forslaget om offentliggørelse af oplysninger om hændelser, som ovenfor beskrevet, er udarbejdet med baggrund i de anbefalinger, som fremgår af Justitsministeriets betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser m.v. I betænkningen anbefales det, at der inden indførelse af ordninger med systematisk offentliggørelse af oplysning om kontrolresultater, afgørelser m.v. på internettet i ikke-anonymiseret form foretages en vurdering af det konkrete behov for offentliggørelse, om offentliggørelse kan forventes konkret at være særligt indgribende for personen, om der er tungtvejende samfundsmæssige hensyn bag offentliggørelsesordningen, om offentliggørelse strider mod de gældende databeskyttelsesretlige regler og de almindelige regler om tavshedspligt, og om der af retssikkerhedsmæssige grunde er opstillet administrative regler for forvaltningsmyndighedens behandling af de enkelte sager.

Erhvervsstyrelsen vil alene offentliggøre afgørelser om fysiske personer i anonymiseret form. Der vil derfor som udgangspunkt ikke blive givet personoplysninger til offentlig-

heden, hvorfor disse afgørelser ikke vil være reguleret af de gældende databeskyttelsesretlige regler. Offentliggørelse af navnet på den berørte operatør vil blive offentliggjort, såfremt Erhvervsstyrelsen vurderer, at det er nødvendigt for at forebygge eller håndtere en igangværende hændelse, medmindre det samme resultat kan nås med en anonymiseret offentliggørelse, som alene omfatter den konkrete hændelse.

Offentliggørelse vil ske efter høring af operatøren, og Erhvervsstyrelsen vil foretage en afvejning af på den ene side offentlighedens interesse i at blive informeret om trusler m.v., herunder om der helt eller delvis ikke er adgang til hjemmesider under et topdomænenavn og på den anden side mulig kommerciel skade samt skade for omdømmet for den pågældende operatør. Det vil særligt være i offentlighedens interesse at få oplysninger om en hændelse, som kan have betydning for at forebygge en gentagelse af hændelsen eller kan bidrage i forbindelse med håndtering af en igangværende hændelse. Det er ikke hensigten, at der skal offentliggøres oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende for så vidt Erhvervsstyrelsen vurderer, at det er af væsentlig betydning for operatøren, eller oplysninger om enkeltpersoners forhold. Center for Cybersikkerhed kan i koordination med Erhvervsstyrelsen stå for offentliggørelsen i de tilfælde, hvor hændelsen vedrører flere af de sektorer, som er omfattet af NIS-direktivet.

Til § 7

Efter den foreslåede § 7 skal en udbyder af en digital tjeneste, der ikke har hovedsæde i EU, men som tilbyder sin tjeneste i Danmark, udpege en repræsentant i Danmark eller i et andet EU-land, hvor tjenesten tilbydes. Bestemmelsen gennemfører dele af artikel 18 i NIS-direktivet og skal sikre, at Erhvervsstyrelsen i spørgsmål om overtrædelse af bestemmelserne i dette lovforslag vil kunne kontakte en repræsentant for den digitale udbyder, hvis digitale udbydere ikke har hjemsted i Danmark.

Med henblik på at afgøre, om udbyderen tilbyder sin digitale tjeneste i Danmark, skal der lægges vægt på, om det er åbenbart, at udbyderen af digitale tjenester påtænker at tilbyde tjenester til personer i Danmark. Alene det forhold, at der i Danmark er adgang til udbyderens eller en mellemmands websted eller til andre kontaktoplysninger er utilstrækkeligt til at fastslå en sådan hensigt. Imidlertid kan faktorer såsom information på dansk, priser angivet i danske kroner eller omtale af kunder eller brugere i Danmark, gøre det åbenbart, at udbyderen påtænker at tilbyde sine digitale tjenester i Danmark. Det er den enkelte udbyder af digitale tjenesters ansvar at udpege en repræsentant, hvis en sådan ikke findes i et andet EU-land.

Repræsentanten skal udtrykkeligt udpeges ved en skriftlig fuldmagt fra udbyderen til at handle på vegne af udbyderen for så vidt angår dennes forpligtelser i medfør af bestemmelserne i dette direktiv, herunder i forbindelse med underretning om hændelser. Udpegelsen af en repræsentant af udbyderen af digitale tjenester berører ikke eventuelle retlige skridt mod selve udbyderen af digitale tjenester.

Til § 8

Den foreslåede § 8 i lovforslaget gennemfører dele af artikel 16 i NIS-direktivet. Med lovforslaget fastlægges sikkerhedskravene for udbydere af digitale tjenester.

Efter lovforslagets *§ 8, stk. 1*, skal udbydere af digitale tjenester identificere og træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i de net- og informationssystemer, som de anvender i forbindelse med deres tjenester. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i mål med risikoen. Udbyderen skal i den forbindelse inddrage: 1) sikkerheden i systemer og faciliteter, 2) håndtering af hændelser, 3) styring af driftskontinuitet, 4) monitorering, audit og testning, og 5) overholdelse af internationale standarder. Bestemmelsen gennemfører artikel 16, stk. 1, i NIS-direktivet.

Efter lovforslagets *§ 8, stk. 2*, skal udbydere af digitale tjenester endvidere træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i deres net- og informationssystemer for at sikre kontinuiteten i disse tjenester. Bestemmelsen gennemfører NIS-direktivets artikel 16, stk. 2.

Bestemmelserne i lovforslagets § 8, stk. 1 og 2, skal ses i sammenhæng. Formålet med begge bestemmelser er lig lovforslagets § 4, stk. 1 og 2, at fremme en risikostyringskultur med risikovurdering og gennemførelse af sikkerhedsforanstaltninger, som står i forhold til risiciene. Det er ligesom for operatører afgørende, at udbyderne ikke pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, hvorfor kravene skal stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende net- og informationssystem, under hensyntagen til sådanne foranstaltningers aktuelle stadie.

Bestemmelserne i lovforslagets § 8, stk. 1 og 2, vil indebære, at udbyderne skal arbejde systematisk og risikobaseret med sikkerheden i deres net- og informationssystemer. Risikostyringsforanstaltningerne vil omfatte foranstaltninger til at identificere alle risici for hændelser, forebygge, detektere og håndtere hændelser og begrænse deres konsekvenser. Hvilke foranstaltninger inden for lovgivningens rammer, der konkret skal træffes, overlades lig hvad der foreslås for operatørerne til udbyderne. Til forskel for lovforslagets § 4 for operatører præciseres det imidlertid i den foreslåede § 8, stk. 1, at udbyderne i deres tilrettelæggelse af deres foranstaltninger skal inddrage følgende elementer: Sikkerheden i systemer og faciliteter, håndtering af hændelser, styring af driftskontinuitet, monitorering, audit (kontrol) og testning samt overholdelse af internationale standarder. Disse elementer er nærmere specificeret i Kommissionens gennemførelsesforordning 2018/151/EU af 30. januar 2018.

Efter lovforslagets *§ 8, stk. 3*, kan Erhvervsstyrelsen fastsætte nærmere regler om foranstaltninger efter stk. 1 og 2. Bemyndigelsen vil skulle anvendes til at præcisere lovforslagets krav i § 8, stk. 1 og 2, om risikostyringsforanstaltninger på baggrund af Kommissionens gennemførelsesforord-

ning 2018/151/EU af 30. januar 2018. Bemyndigelsen kan fx anvendes til at fastsætte bestemmelser om adgang til fysisk- og miljømæssig sikkerhed såsom beskyttelse mod indbrud og brand, samt bestemmelser om forsyningssikkerhed såsom udarbejdelse af politikker for adgang til elforsyning. Bemyndigelsen vil ikke blive anvendt til at fastsætte yderligere krav end de krav, der følger af NIS-direktivet. Endvidere vil der i udmøntningen af bemyndigelsen blive lagt vægt på at sikre, at udbyderne kun underlægges proportionale krav, der i videst muligt omfang overlader et skøn til udbyderne til selv at beslutte indholdet af deres sikkerhedsforanstaltninger.

Til § 9

Den foreslåede § 9 i lovforslaget gennemfører dele af artikel 16 i NIS-direktivet. Med lovforslaget fastlægges udbyderes forpligtelse til at underrette myndighederne i tilfælde af hændelser.

Efter lovforslagets *§ 9, stk. 1*, skal udbydere af digitale tjenester hurtigst muligt underrette Erhvervsstyrelsen og Center for Cybersikkerhed om hændelser, der har betydelige konsekvenser for leveringen af deres tjeneste. Underretningen skal indeholde oplysninger, der gør det muligt for Erhvervsstyrelsen og Center for Cybersikkerhed at vurdere de eventuelle grænseoverskridende konsekvenser ved hændelsen, jf. dog stk. 3.

Hændelser defineres her i overensstemmelse med lovforslagets § 2, nr. 7, hvorefter en hændelse er enhver begivenhed, der har egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.

Med hurtigst muligt sigtes til, at udbyderen under hensyntagen til arbejdet med at minimere konsekvenserne af hændelsen skal foretage underretningen, så snart denne har de nødvendige oplysninger til at kunne vurdere omfanget af hændelsen. Det gælder særligt, hvis hændelsen vurderes at kunne påvirke flere udbydere eller til at være grænseoverskridende. Bliver Erhvervsstyrelsen bekendt med, at der ikke er foretaget underretning af en hændelse, som har væsentlige konsekvenser, vil der som udgangspunkt blive udstedt et påbud om at foretage underretningen. Manglende opfyldelse af påbuddet er straffebelagt, jf. lovforslagets § 17.

Efter lovforslagets *§ 9, stk. 2*, skal udbydere i vurderingen af, om en hændelse har væsentlige konsekvenser, inddrage navnlig: a) antallet af brugere, der er berørt af hændelsen, b) hændelsens varighed, c) hvor stort et geografisk område, der er berørt af hændelsen, d) omfanget af afbrydelsen af tjenestens funktion, og e) omfanget af konsekvenserne for økonomiske og samfundsmæssige aktiviteter. De nævnte kriterier vil skulle forstås i overensstemmelse med Kommissionens gennemførelsesforordning 2018/151/EU af 30. januar 2018.

I henhold til lovforslagets *§ 9, stk. 3*, skal underretning efter stk. 1 kun ske, i det omfang udbyderen af digitale tjenester har adgang til relevante oplysninger, herunder oplysninger omfattet af stk. 2. Med bestemmelsen vil udbyderen ikke skulle underrette myndighederne, hvis ikke udbyderen har de oplysninger, der er nødvendige for at fastlægge om en hændelse har væsentlige konsekvenser. Det forhold, at udbyderen ikke har adgang til oplysninger om alle de nævnte kriterier i stk. 2, fx antal brugere, medfører ikke, at udbyderens forpligtelse til at underrette bortfalder alene af den grund. Udbyderen vil således skulle foretage en samlet vurdering af de oplysninger, der er til rådighed, og på den baggrund foretage en vurdering af hændelsens væsentlighed.

De nærmere kriterier for, hvornår og hvordan en underretning vil skulle ske samt indholdet af underretningen, vil blive fastlagt af Erhvervsstyrelsen i henhold til bemyndigelsesbestemmelsen i lovforslagets *§ 9, stk. 4*. Bemyndigelsen vil blive anvendt til at præcisere kriterierne for, hvornår en hændelse skal indberettes på baggrund af Kommissionens gennemførelsesforordning 2018/151/EU af 30. januar 2018. Bemyndigelsen vil endvidere anvendes til at præcisere, hvordan indberetningen skal foregå – fx gennem en fælles indberetningsløsning på virk.dk.

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 unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet, jf. persondataforordningens art. 33, stk. 1.

Til § 10

Den foreslåede § 10 i lovforslaget gennemfører dele af artikel 16 i NIS-direktivet.

Med bestemmelsen i stk. 1 foreslås det, at Erhvervsstyrelsen kan videregive oplysninger til Center for Cybersikkerhed om hændelser, der er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver som nationalt centralt kontaktpunkt i henhold til NIS-direktivet. Bestemmelsen skal anvendes i overensstemmelse med forvaltningslovens § 28 og under iagttagelse af de grundlæggende principper om saglighed og proportionalitet. 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. Center for Cybersikkerhed skal i henhold til direktivet foretage monitorering af hændelser på nationalt plan, tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser, at reagere på hændelser, udarbejdelse af dynamisk risiko- og hændelsesanalyser og situationsrapporter. Center for Cybersikkerhed vil endvidere skulle orientere kontaktpunkter i andre medlemsstater om hændelser, der har betydelige konsekvenser for leveringen af de tjenester, der udbydes i de pågældende lande. Orienteringen vil ske under hensyntagen til udbyderens sikkerhed og kommercielle interesser samt krav på fortrolig behandling af oplysninger.

Med bestemmelsen i *stk. 2* foreslås det, at Erhvervsstyrelsen efter høring af udbyderen af digitale tjenester kan oplyse

offentligheden om konkrete hændelser eller kræve, at udbyderen af digitale tjenester offentliggør det, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse i øvrigt er i offentlighedens interesse. Det vil særligt være i offentlighedens interesse at få oplysninger om en hændelse, som kan have betydning for at forebygge en gentagelse af hændelsen eller kan bidrage i forbindelse med håndtering af en igangværende hændelse.

Erhvervsstyrelsens beslutning om at offentliggøre en konkret hændelse er ikke en afgørelse i forvaltningslovens forstand. Forslaget om offentliggørelse af oplysninger om hændelser, som ovenfor beskrevet, er udarbejdet med baggrund i de anbefalinger, som fremgår af Justitsministeriets betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser m.v. I betænkningen anbefales det, at der inden indførelse af ordninger med systematisk offentliggørelse af oplysning om kontrolresultater, afgørelser m.v. på internettet i ikke-anonymiseret form foretages en vurdering af det konkrete behov for offentliggørelse, om offentliggørelse kan forventes konkret at være særligt indgribende for personen, om der er tungtvejende samfundsmæssige hensyn bag offentliggørelsesordningen, om offentliggørelse strider mod de databeskyttelsesretlige regler og de almindelige regler om tavshedspligt, og om der af retssikkerhedsmæssige grunde er opstillet administrative regler for forvaltningsmyndighedens behandling af de enkelte sager.

Erhvervsstyrelsen vil alene offentliggøre afgørelser om fysiske personer i anonymiseret form. Der vil derfor som udgangspunkt ikke blive givet personoplysninger til offentligheden, hvorfor disse afgørelser ikke vil være reguleret af de gældende databeskyttelsesretlige regler. Offentliggørelse af navnet på den berørte operatør vil blive offentliggjort, såfremt Erhvervsstyrelsen vurderer, at det er nødvendigt for at forebygge eller håndtere en igangværende hændelse, medmindre det samme resultat kan nås med en anonymiseret offentliggørelse, som alene omfatter den konkrete hændelse.

Offentliggørelse vil ske efter høring af udbyderen, og der skal foretages en afvejning af på den ene side offentlighedens interesse i at blive informeret om trusler og på den anden side mulig imageskade og kommerciel skade for den pågældende udbyder. Det er ikke hensigten, at der skal offentliggøres oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende for så vidt Erhvervsstyrelsen vurderer, at det er af væsentlig betydning for udbyderen, eller oplysninger om enkeltpersoners forhold. Center for Cybersikkerhed kan i koordination med Erhvervsstyrelsen stå for offentliggørelsen i de tilfælde, hvor hændelsen vedrører flere af de sektorer, som er omfattet af NIS-direktivet.

Til § 11

Med lovforslagets *§ 11, stk. 1*, skabes der hjemmel til, at Erhvervsstyrelsen kan fastsætte regler om, at skriftlig kommunikation til og fra styrelsen om alle forhold skal foregå digitalt.

Lovforslaget indebærer bl.a., at skriftlige henvendelser m.v. til styrelsen om forhold, som er omfattet af loven eller regler udstedt i medfør af loven, ikke anses for behørigt modtaget i styrelsen, hvis de indsendes på anden vis end den foreskrevne digitale måde.

Samtidig indebærer lovforslaget, at meddelelser m.v. til eller fra Erhvervsstyrelsen, der sendes på den foreskrevne digitale måde, anses for at være kommet frem til modtageren på det tidspunkt, hvor meddelelsen m.v. er tilgængelig digitalt for modtageren, jf. det foreslåede stk. 3. Det vil sige med samme retsvirkninger som fysisk post, der anses for at være kommet frem, når den pågældende meddelelse m.v. er lagt i adressatens fysiske postkasse.

Af bekendtgørelsen, som udmønter den foreslåede bemyndigelse, vil det komme til at fremgå, hvem der omfattes af pligten til at kommunikere digitalt med styrelsen, om hvilke forhold og på hvilken måde.

Ved henvendelser til styrelsen kan styrelsen stille krav om, at den pågældende oplyser en e-mailadresse, som den pågældende kan kontaktes på i forbindelse med behandlingen af en konkret sag eller henvendelse til styrelsen. I den forbindelse kan der også pålægges den pågældende en pligt til at underrette styrelsen om en eventuel ændring i e-mailadressen, inden den konkrete sag afsluttes eller henvendelsen besvares, medmindre e-mails automatisk bliver videresendt til den nye e-mailadresse.

I bekendtgørelsen, som udmønter den foreslåede bemyndigelse i stk. 1, kan der fastsættes regler om, at Erhvervsstyrelsen kan sende visse meddelelser, herunder afgørelser og påbud m.v., til adressatens digitale postkasse med de retsvirkninger, der følger af Lov om Offentlig Digital Post.

I bekendtgørelsen kan der desuden fastsættes regler om fritagelse for pligten til digital kommunikation. Da der er tale om kommunikation om erhvervsforhold, vil fritagelsesmuligheden blive stærkt begrænset. Fritagelsesmuligheden tænkes navnlig anvendt, hvor det er påkrævet at anvende en dansk digital signatur, og der er tale om en person uden dansk CPR-nummer eller en virksomhed med hjemsted i udlandet, som ikke kan få en dansk digital signatur.

Fritagelsesmuligheden kan endvidere tænkes anvendt, hvis materialet på grund af sin særlige beskaffenhed ikke er egnet til digital fremsendelse. Det kan fx være tilfældet i forbindelse med en undersøgelsessag, hvor der kan være tale om udveksling af en meget omfattende mængde dokumentation m.v.

Det forhold, at en virksomhed eller en person oplever, at den pågældendes egen computer ikke fungerer, at den pågældende har mistet koden til sin digitale signatur eller oplever lignende hindringer, som det er op til den pågældende at overkomme, kan ikke føre til fritagelse for pligten til digital kommunikation. Efter det foreslåede *stk. 2* kan der i bekendtgørelsen specificeres krav om anvendelse af bestemte it-systemer, digitale formater og digital signatur eller lignende.

Det foreslåede *stk. 3* fastsætter, hvornår en digital meddelelse må anses for at være kommet frem til adressaten for

meddelelsen, dvs. modtageren af meddelelsen. For meddelelser, der sendes til en myndighed, er myndigheden adressat for meddelelsen. For meddelelser, som myndigheden sender, er den pågældende virksomhed etc., som meddelelsen sendes til, adressat for meddelelsen.

En meddelelse vil normalt anses for at være kommet frem til en myndighed på det tidspunkt, hvor meddelelsen er tilgængelig for myndigheden, dvs. når styrelsen kan behandle meddelelsen. Dette tidspunkt vil normalt blive registreret automatisk i en modtagelsesanordning eller et datasystem. Har myndigheden fastsat en senest dato for modtagelse af en meddelelse, betragtes meddelelsen som været rettidigt kommet frem, når meddelelsen er registreret modtaget inden midnat den pågældende dato. En meddelelse vil normalt anses for at være kommet frem til en virksomhed eller person på det tidspunkt, hvor meddelelsen er tilgængelig for den pågældende. En meddelelse vil blive anset for at være tilgængelig, selvom den pågældende ikke kan skaffe sig adgang til meddelelsen, hvis dette skyldes hindringer, som det er op til den pågældende at overkomme. Som eksempler herpå kan nævnes, at den pågældendes egen computer ikke fungerer, eller den pågældende har mistet koden til sin digitale signatur.

Til § 12

Med lovforslagets *§ 12* kan der fastsættes regler om, at Erhvervsstyrelsen kan udstede afgørelser og andre dokumenter efter denne lov eller regler udstedt i medfør af denne lov uden underskrift, med maskinel eller på tilsvarende måde gengivet underskrift eller under anvendelse af en teknik, der sikrer entydig identifikation af den, som har udstedt afgørelsen eller dokumentet. Bestemmelsen og regler udstedt i medfør heraf finder anvendelse under iagttagelse af identifikationskravet i forvaltningslovens § 32 b.

Til § 13

Den foreslåede § 13 vedrører dokumenter, som er omfattet af denne lov eller forskrifter udstedt i medfør heraf, og som er udstedt af andre end en myndighed, hvor det efter loven eller regler udstedt i medfør af loven er krævet, at dokumentet er underskrevet. Underskriftskravet kan fremgå udtrykkeligt eller forudsætningsvist af de pågældende regler.

For at der ikke skal kunne opstå tvivl om, at underskriftskravet kan opfyldes på anden måde end ved en personlig underskrift, foreslås det, at der indsættes en udtrykkelig bestemmelse i loven om, at underskriftskravet som anført i *stk. 1* kan opfyldes ved, at underskriveren anvender en teknik, der sikrer entydig identifikation af den pågældende, fx digital signatur.

Det foreslås i *stk. 2*, at Erhvervsstyrelsen kan fastsætte nærmere regler om, hvordan kravet om personlig underskrift kan fraviges. Med hjemmel i den foreslåede bestemmelse kan der desuden fastsættes regler om, at krav om personlig underskrift ikke kan fraviges for visse typer af dokumenter.

Til § 14

Den foreslåede § 14 har til formål at skabe rammerne for et tilsyn med operatørernes og udbydernes overholdelse af kravene til informationssikkerhed. Bestemmelsen gennemfører dele af NIS-direktivets artikel 15 og 17.

Med bestemmelsen i *stk. 1* foreslås det, at Erhvervsstyrelsen fører tilsyn med overholdelsen af loven og regler udstedt i medfør af loven. Hvad der nærmere ligger i tilsynsforpligtelsen bliver udbygget i stk. 2 og 3.

Efter det foreslåede *stk.* 2 kan Erhvervsstyrelsen kræve, at operatører og udbydere afgiver de oplysninger, der er nødvendige for styrelsens tilsyn efter loven. Erhvervsstyrelsen sikres med bestemmelsen adgang til enhver oplysning, der er nødvendige til gennemførelse af styrelsens tilsynsvirksomhed. Sådanne oplysninger kan eksempelvis være til brug for identificeringen af operatører af væsentlige tjenester samt i forhold til at indhente operatørers eller udbyderes informationssikkerhedspolitik, risikovurderinger, beredskabsplaner, netarkitektur- og designdokumenter samt testrapporter.

Efter det foreslåede *stk. 3* kan Erhvervsstyrelsen endvidere som led i sit tilsyn med operatører af væsentlige tjenester kræve dokumentation af operatørerne for den faktiske gennemførelse af sikkerhedspolitikker. På baggrund af en risikoanalyse skal operatører af væsentlige tjenester således kunne dokumentere at have opbygget, vedligeholdt og gennemført sikkerhedspolitikker, der er godkendt af ledelsen. Sikkerhedspolitikkerne bør angive de strategiske mål og beskrive den sikkerhedsstyring, som operatøren har. Endvidere bør de indeholder alle relevante sikkerhedselementer i forhold til fx sikkerhedsgodkendelsesprocesser, sikkerhedsrevision, kryptering, sikkerhedsvedligeholdelse og hændelseshåndtering. Der fastsættes ingen krav til, hvordan dokumentation skal forelægges, ud over at den skal foreligge elektronisk, men den skal på overskuelig vis dokumentere den faktiske gennemførelse af sikkerhedspolitikker, herunder redegøre for gennemførelsen af relevante sikkerhedselementer.

Hvis Erhvervsstyrelsen på baggrund af de oplysninger, styrelsen modtager som led i sit tilsyn, konstaterer, at en operatør eller en udbyder ikke har efterlevet kravene til sikkerhedsforanstaltninger og underretning af hændelser efter denne lov, kan styrelsen efter det foreslåede *stk. 4*, påbyde udbydere og operatører, at de afhjælper de pågældende mangler. Et påbud kan fx indebære, at der skal gennemføres en risikoanalyse, eller at der skal gennemføres passende foranstaltninger på baggrund af en gennemført risikoanalyse. Et eventuelt påbud vil typisk først blive udstedt efter en indledende dialog, og hvis virksomheden m.v. ikke selv afhjælper en konstateret mangel inden for en rimelig tid. Såfremt det konstateres, at der ikke er gennemført en risikoanalyse, vil et påbud typisk blive udstedt ved konstateringen heraf med en rimelig fastsat tidramme for at få gennemført en risikoanalyse og de fornødne sikkerhedsforanstaltninger.

Til § 15

Med den foreslåede § 15 vil Erhvervsstyrelsen skulle offentliggøre alle afgørelser, hvori påbud udstedes.

Det foreslåede *stk. 1, 1. pkt*., medfører, at offentliggørelsen af afgørelsen skal ske på Erhvervsstyrelsens hjemmeside. Offentliggørelsen vil ske efter, at den fysiske eller juridiske person er blevet underrettet om afgørelsen. Erhvervsstyrelsen kan bestemme, om hele afgørelsen eller kun dele af afgørelsen skal offentliggøres, eventuelt i form af et resumé. Dog skal Erhvervsstyrelsens pålagte påbud og overtrædelsens art offentliggøres. Offentliggørelsen af oplysningerne vil være tilgængelig på styrelsens hjemmeside i mindst fem år efter offentliggørelsen. Erhvervsstyrelsen er ikke forpligtet til efter forvaltningslovens § 19 at iværksætte en partshøring forud for offentliggørelsen, idet beslutningen om offentliggørelse sker som led i faktisk forvaltningsvirksomhed. Beslutning om offentliggørelse betragtes ikke som en afgørelse og kan ikke indbringes for anden administrativ myndighed.

Det foreslås i *stk. 1, 2. pkt*., at offentliggørelse af afgørelser, hvori en fysisk person pålægges et påbud efter den foreslåede § 14, stk. 4, anonymiseres for så vidt angår personoplysninger, herunder identiteten på den fysiske person. Forslaget om offentliggørelse af afgørelser, hvori påbud udstedes, er udarbejdet med baggrund i de anbefalinger, som fremgår af Justitsministeriets betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser m.v. I betænkningen anbefales det, at der inden indførelse af ordninger med systematisk offentliggørelse af oplysning om kontrolresultater, afgørelser m.v. på internettet i ikke-anonymiseret form foretages en vurdering af det konkrete behov for offentliggørelse, om offentliggørelse kan forventes konkret at være særligt indgribende for personen, om der er tungtvejende samfundsmæssige hensyn bag offentliggørelsesordningen, om offentliggørelse strider mod de gældende databeskyttelsesretlige regler og de almindelige regler om tavshedspligt, og om der af retssikkerhedsmæssige grunde er opstillet administrative regler for forvaltningsmyndighedens behandling af de enkelte sager.

Den offentlige og private sektor er – indtil den 24. maj 2018 – omfattet af Lov nr. 429 af 31. maj 2000 med senere ændringer (herefter Persondataloven) og tilhørende bekendtgørelser, når der behandles personoplysninger. Persondataloven gennemfører databeskyttelsesdirektivet, som ophæves pr. 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. forslagets § 46, stk. 2.

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, der regulerer området for behandling af personoplysninger.

En offentliggjort afgørelse vil derfor ikke indeholde personoplysninger, hvorfor disse afgørelser ikke vil være reguleret af de gældende databeskyttelsesretlige regler. En afgørelse vil dermed ikke indeholde oplysninger om en person, der direkte eller indirekte kan identificere personen, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Offentliggørelse af påbud, som pålægges en fysisk person, skal således ikke indeholde oplysning om identiteten af den fysiske person. Formålet er, at den fysiske person ikke må kunne identificeres. Det tilsikres hermed, at der ikke sker en offentliggørelse af personoplysninger, idet offentliggørelse af, at fysiske personer har modtaget et påbud, vil ske i anonymiseret form. Da enkeltmandsvirksomheder normalt drives af en fysisk person, vil der tilsvarende skulle ske anonymisering af navnet på en enkeltmandsvirksomhed svarende til, hvad der gælder for fysiske personer.

Erhvervsstyrelsen vil ved hver enkelt offentliggørelse af oplysninger om, at en fysisk person har modtaget et påbud, overveje, om offentliggørelsen indeholder oplysninger, der er personhenførbare. Oplysninger om, at den fysiske person, som har modtaget påbuddet, arbejder i en bestemt afdeling, har en bestemt stilling eller udfører bestemte funktioner kan efter omstændighederne udgøre personoplysninger i henhold til de databeskyttelsesretlige regler, hvis det fra disse oplysninger sammenholdt med andre offentliggjorte oplysninger er muligt at identificere personen.

Det foreslås efter *stk. 2*, at afgørelser vedrørende en juridisk person offentliggøres med identiteten på den juridiske person, medmindre offentliggørelsen af identiteten vil være til skade for en igangværende strafferetlig efterforskning eller offentliggørelsen vil forvolde uforholdsmæssig stor skade. Udgangspunktet er således for juridiske personer, at et påbud offentliggøres med oplysning om navnet på den juridiske person. Der foreligger dog undtagelser til dette.

For det første skal identiteten på den juridiske person ske i anonymiseret form af hensyn til en igangværende strafferetlig efterforskning. Beslutning om offentliggørelse bør alene ske efter høring af den relevante politimyndighed, dog således at der eventuelt kan indgås en mere generel aftale om offentliggørelse af visse sagstyper. Ved tvivl forelægges spørgsmålet om offentliggørelse for den relevante politimyndighed.

For det andet kan anonymisering ske, hvis offentliggørelsen vil forvolde uforholdsmæssig stor skade, fx for den juridiske person, afgørelsen vedrører, investorer eller andre. Det forhold, at offentliggørelse af en juridisk persons navn vil kunne medføre tab af kunder, eller at offentliggørelse vil

kunne bane vej for et erstatningskrav mod den juridiske person, vil ikke i sig selv være tilstrækkeligt til, at offentliggørelse skal ske i anonymiseret form. Undtagelsen bør således kun finde anvendelse på de tilfælde, hvor den juridiske persons fortsatte drift vil blive truet, eller hvis meget væsentlige interesser krænkes.

Da udkast til Erhvervsstyrelsens afgørelser i deres helhed sendes i partshøring hos de berørte juridiske personer, vil de berørte virksomheder i forbindelse med høringen få mulighed for at kommentere på spørgsmålet om offentliggørelse, herunder hvis det indstilles, at afgørelsen offentliggøres med angivelse af identiteten på operatøren eller udbyderen, hvilket er det altovervejende udgangspunkt. Beslutningen om at offentliggøre virksomhedens navn er endelig og kan således ikke indbringes for højere administrativ myndighed.

Det foreslås i *stk. 3*, at anonymisering af identiteten på en juridisk person sker efter 2 år regnet fra og med datoen for offentliggørelsen. Herved skabes der klarhed over, hvor lang tid en offentliggørelse vil være tilgængelig i ikke-anonymiseret form.

Til § 16

Med den foreslåede § 16 kan Erhvervsstyrelsens afgørelser efter § 14, stk. 2, 3 og 4, ikke indbringes for anden administrativ myndighed. Bestemmelsen afskærer den administrative klageadgang fra Erhvervsstyrelsen til erhvervsministeren.

Baggrunden for den foreslåede bestemmelse er, at de afgørelser, som Erhvervsstyrelsen vil træffe efter loven, vil være af teknisk karakter og forudsætter betydelig teknisk indsigt på området, som det ikke kan forventes, at Erhvervsministeriets departement er i besiddelse af. Der kan således fx være tale om afgørelser om, at operatører af væsentlige tjenester ikke har truffet de nødvendige foranstaltninger for at styre risiciene for sikkerheden i deres net- og informationssystemer. At træffe disse afgørelser vil forudsætte betydelig it-sikkerhedsmæssig indsigt på området, som det ikke kan forventes, at ministeriets departement er i besiddelse af. Erhvervsstyrelsen vil efter lovforslaget altid skulle træffe afgørelser, der kræver teknisk indsigt.

Erhvervsministeriets departement vil ikke kunne foretage en realitetsbehandling af eventuelle klager over Erhvervsstyrelsens beslutning om offentliggørelse efter § 15, stk. 1, idet beslutningen er udtryk for faktisk forvaltningsvirksomhed.

Bestemmelsen berører dog ikke den almindelige adgang til at få afgørelser prøvet ved domstolene.

Til § 17

Bestemmelsen har til formål at gennemføre artikel 21 i NIS-direktivet, hvorefter medlemsstaterne forpligtes til at fastsætte sanktioner for overtrædelse af de nationale regler, der vedtages i medfør af NIS-direktivet.

Efter det foreslåede *stk. 1*, vil operatører af tjenester og udbydere af digitale tjenesters undladelse af at efterkomme Erhvervsstyrelsens krav om at afgive oplysninger, der er nødvendige for styrelsens tilsyn efter § 14, stk. 2, kunne straffes med bøde. Desuden forslås det, at operatører af væsentlige tjenester, der undlader at efterkomme Erhvervsstyrelsens krav om dokumentation efter § 14, stk. 3, vil kunne straffes med bøde. Endvidere foreslås det, at operatører af væsentlige tjenester og udbydere af digitale tjenesters undladelse af at efterkomme Erhvervsstyrelsens påbud efter § 14, stk. 4, kan straffes med bøde.

Erhvervsministeren bemyndiges med det foreslåede *stk. 2* til at fastsætte straf i form af bøde for overtrædelse af bestemmelser i regler, som udfærdiges i medfør af § 3, stk. 3, § 4, stk. 3 eller § 5, stk. 4, samt Erhvervsstyrelsen bemyndiges til at fastsætte straf i form af bøde for overtrædelse af bestemmelser i regler, som udfærdiges i medfør af § 8, stk. 3 eller § 9, stk. 4.

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

Til § 18

Bestemmelsen fastsætter tidspunktet for lovens ikrafttræden.

I medfør af NIS-direktivets artikel 25, skal medlemsstaterne vedtage og offentliggøre de love og administrative bestemmelser, der er nødvendige for at efterkomme direktivet, senest den 9. maj 2018.

Det foreslås derfor, at loven træder i kraft den 10. maj 2018 i overensstemmelse med NIS-direktivet.

Til § 19

Til nr. 1

Med den foreslåede ændring af fodnoten til lov om finansiel virksomhed indsættes en henvisning til, at der med denne lov foretages en gennemførelse af 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, idet lovforslaget implementerer de dele af direktivet i lov om finansiel virksomhed, der omfatter penge- og realkreditinstitutter.

Til nr. 2

I medfør af § 71 i lov om finansiel virksomhed skal en finansiel virksomhed have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger på it-området.

I medfør af § 71, stk. 2, i lov om finansiel virksomhed, kan Finanstilsynet fastsætte nærmere regler om de foranstaltninger, som en finansiel virksomhed skal træffe for at have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger på it-området. Denne bemyndigelse er bl.a. udnyttet ved bekendtgørelse nr.

1026 af 30. juni 2016 om ledelse og styring af pengeinstitutter m.fl. (herefter kaldet ledelsesbekendtgørelsen), hvoraf bekendtgørelsens bilag 5 stiller nærmere krav til it-sikkerhed.

Det følger bl.a. af ledelsesbekendtgørelsens bilag 5, at bestyrelsen skal beslutte en it-sikkerhedspolitik for virksomheden, som ud fra den ønskede risikoprofil på it-området skal indeholde en overordnet stillingtagen til alle væsentlige forhold vedrørende it-sikkerheden. Hvad der er væsentligt, afhænger bl.a. af virksomhedens størrelse samt omfanget og kompleksiteten af virksomhedens it-anvendelse.

NIS-direktivets sikkerhedskrav i artikel 14, stk. 1 og 2, vurderes ikke, at række videre end den nugældende § 71 i lov om finansiel virksomhed og tilhørende ledelsesbekendtgørelse, herunder ledelsesbekendtgørelsens bilag 5. NIS-direktivets sikkerhedskrav vurderes således at være indeholdt i § 71 og i ledelsesbekendtgørelses bilag 5.

NIS-direktivets artikel 14, stk. 3 og 4, indeholder imidlertid også krav om, 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 de væsentlige tjenester, som de leverer. En hændelse forstås som værende enhver begivenhed, der har en negativ indvirkning på sikkerheden i en virksomheds net- og informationssystemer. Med sikkerhed i net- og informationssystemer forstås net- og informationssystemernes 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.

Det fremgår endvidere af NIS-direktivets artikel 14, stk. 3, at underretningen skal indeholde oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. En underretning gør ikke den underrettende part til genstand for et øget ansvar.

Endelig fremgår det af direktivets artikel 14, stk. 4, at med henblik på at fastlægge omfanget af en hændelses konsekvenser, tages det i betragtning, hvor mange brugere, som berøres af afbrydelsen af den væsentlige tjeneste, hændelsens varighed, den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen og om eventuelle grænseoverskridende konsekvenser af hændelsen.

Med henblik på at implementere artikel 14, stk. 3 og 4, foreslås det at udvide § 71, stk. 2, i lov om finansiel virksomhed, således at Finanstilsynet kan fastætte nærmere regler om hændelsesrapportering ved eventuelle hændelser, herunder fastsætte nærmere regler om krav om underretning af Finanstilsynet og Center for Cybersikkerhed ved en hændelse, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer.

Med den foreslåede indførelse af *§ 71, stk. 2, 2. pkt.,* vil Finanstilsynet i bilag 5 til ledelsesbekendtgørelsen kunne fastsætte nærmere regler om hændelsesrapportering ved eventuelle hændelser, herunder fastsætte nærmere regler om krav om underretning af både Finanstilsynet og Center for Cybersikkerhed, som forventes udpeget som CSIRT, ved en hændelse, der har en negativ indvirkning på sikkerheden i en virksomheds net- og informationssystemer. Det skal i den forbindelse bemærkes, at der forventes etableret en fælles indberetningsløsning – fx gennem en fælles portal på virk.dk – hvorigennem alle operatører omfattet af NIS-direktivet vil kunne indberette. Med denne fælles indberetningsløsning forventes en afrapportering til både Finanstilsynet og Center for Cybersikkerhed dermed ikke at have økonomiske konsekvenser for de enkelte omfattede virksomheder.

Finanstilsynet forventes at udnytte bemyndigelsen i den foreslåede § 71, stk. 2, 2. pkt., til at fastsætte nærmere krav om underretninger fra en operatør af væsentlige tjenester til Finanstilsynet og til Center for Cybersikkerhed, i sin egenskab af CSIRT, når der er tale om hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester som virksomheden leverer og som er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

Forpligtelsen til at underrette om hændelser, som har væsentlige konsekvenser for kontinuiteten af de tjenester, som de udpegede operatører af væsentlige tjenester leverer, vil således alene omfatte operatører af væsentlige tjenester, i overensstemmelse med NIS-direktivets artikel 5, stk. 2, hvoraf følger tre kriterier for identificering af en operatør af væsentlige tjenester. Disse kriterier er, når den pågældende virksomhed leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter, og leveringen af denne tjeneste afhænger af net- og informationssystemer, og en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste. Endvidere fremgår det af NIS-direktivets præambel nr. 28, at med henblik på at fastslå hvorvidt en hændelse vil have en forstyrrende virkning på leveringen af en tjeneste, bør medlemsstaterne i tillæg til tværsektorielle forhold også tage højde for sektorspecifikke forhold.

I medfør af NIS-direktivets artikel 5, stk. 5, udarbejder hver medlemsstat mindst hvert andet år efter den 9. maj 2018 en liste over identificerede operatører af væsentlige tjenester, og ajourfører hvis relevant.

I medfør af den foreslåede § 307 a, skal Finanstilsynet udpege de penge- og realkreditinstitutter, der er operatører af væsentlige tjenester, mindst hvert andet år, ud fra de kriterier der følger af forslaget til § 307 a, stk. 2. Finanstilsynet skal således lægge vægt på, at de tjenester, der leveres, er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af tjenesten afhænger af net- og informationssystemer, og at en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten.

For så vidt angår de hændelser, som en operatør af en væsentlig tjeneste skal rapportere om, forstås en hændelse som værende enhver begivenhed, der har en negativ indvirkning

på sikkerheden i virksomhedens net- og informationssystemer. Med sikkerhed i net- og informationssystemer forstås net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

Som et eksempel på en hændelse, som en operatør af en væsentlig tjeneste skal rapportere om, kunne blandt andet tænkes at en bank bliver ramt af et hackerangreb, som betyder, at mange systemer, der normalt anvendes af både privatkunder i hele Danmark og interne i banken, ikke længere kan anvendes.

Et andet tænkt eksempel kunne være, at der under en større systemopdatering i en bank, sker en teknisk fejl, som betyder at der ikke kan gennemføres transaktioner på tværs af landegrænser i flere dage. Disse manglende transaktioner vil kunne have store konsekvenser både økonomisk og samfundsmæssigt, eftersom brugere ikke vil have mulighed for at styre transaktionerne.

Ovenstående eksempler skal ikke forstås som en udtømmende liste. I tilfælde af en hændelse vil det således kræve at den enkelte virksomhed foretager en konkret vurdering af om der er tale om en hændelse, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som virksomheden leverer og som er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

En hændelses konsekvenser fastlægges navnlig ud fra 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. For at Finanstilsynet og Center for Cybersikkerhed, som national CSIRT, kan vurdere en hændelses konsekvenser, skal underretningerne indeholde oplysninger, der gør det muligt at fastslå hændelsens omfang og herunder eventuelle grænseoverskridende konsekvenser for hændelsen.

Det forventes derfor fastsat på bekendtgørelsesniveau i medfør af den foreslåede § 71, stk. 2, 2. pkt., at en underretning skal indeholde oplysninger om antallet af brugere, som berøres af afbrydelsen af den væsentlige tjeneste, oplysninger om hændelsens varighed, oplysninger om den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen, og oplysninger om eventuelle grænseoverskridende konsekvenser af hændelsen.

Til nr. 3

Forslaget til *§ 307 a*, gennemfører NIS-direktivets artikel 5, stk. 1-3, og stk. 5, hvorefter medlemsstaterne senest den 9. november 2018 identificerer operatører af væsentlige tjenester ud fra, at de tjenester der leveres er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af tjenesterne afhænger af net- og informationssystemer, og at en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesterne.

Med en hændelse forstås enhver begivenhed, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer. Med sikkerhed i net- og informationssystemer forstås net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

Det følger endvidere af direktivets artikel 5, stk. 5, at listen over identificerede operatører af væsentlige tjenester tages op til revision mindst hvert andet år og ajourføres hvis relevant.

Med den foreslåede *§ 307 a, stk. 1*, skal Finanstilsynet mindst hvert andet år udpege de penge- og realkreditinstitutter, der er operatører af væsentlige tjenester. Dermed skal Finanstilsynet mindst hvert andet år offentliggøre en liste over de penge- og realkreditinstitutter, der er operatører af væsentlige tjenester. Det indebærer at listen skal ajourføres løbende og mindst hvert andet år. Det forventes at Finanstilsynet vil offentliggøre en liste første gang primo november 2018 i overensstemmelse med NIS-direktivets artikel 5, stk. 1.

Med den foreslåede *§ 307 a, stk. 2*, skal Finanstilsynet i forbindelse med udpegningen efter stk. 1, lægge vægt på tre kriterier.

Finanstilsynet skal for det første lægge vægt på, at penge- og realkreditinstitutterne udbyder tjenester, som er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

Finanstilsynet skal for det andet lægge vægt på, at de pågældende penge- og realkreditinstitutters levering af tjenesterne afhænger af net- og informationssystemer.

Endelig skal Finanstilsynet for det tredje lægge vægt på, at en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesterne.

Med den foreslåede *§ 307 a, stk. 3, 1. pkt.*, kan Finanstilsynet fastsætte nærmere regler om identificeringen af operatører af væsentlige tjenester. Finanstilsynet vil dermed kunne fastsætte nærmere regler for udpegningen efter stk. 1, herunder nærmere fastsætte hvilke kriterier, der skal være opfyldt, for at et penge- eller realkreditinstitut udpeges som en operatør af væsentlige tjenester.

Bemyndigelsen i § 307 a, stk. 3, 1. pkt., vil bl.a. blive udnyttet på bekendtgørelsesniveau.

I medfør af det foreslåede § 307 a, stk. 3, 2. pkt., vil Finanstilsynet ligeledes udarbejde en liste over tjenester, som penge- og realkreditinstitutter leverer, der anses for at være væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter. Dette betyder, at et penge- eller realkreditinstitut, der bliver udpeget som operatør af væsentlige tjenester, kan holde de væsentlige tjenester adskilt fra de ikke-væsentlige tjenester.

Til nr. 4

I medfør af § 354, stk. 1, i lov om finansiel virksomhed er Finanstilsynets ansatte underlagt en særlig tavshedspligt. Finanstilsynets ansatte er således under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger.

§ 354, stk. 6, i lov om finansiel virksomhed fastsætter i hvilke tilfælde og til hvem Finanstilsynet kan videregive fortrolige oplysninger, uanset § 354, stk. 1.

§ 354 i lov om finansiel virksomhed gennemfører artikel 53-60 i Europa-Parlamentets og Rådets Direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber (CRD IV).

Bestemmelsen indeholder hovedreglen om Finanstilsynets tavshedspligt og er en særbestemmelse om tavshedspligt, jf. offentlighedslovens § 35. Det indebærer, at der ikke vil være mulighed for adgang til aktindsigt efter offentlighedsloven i oplysninger hos Finanstilsynet, der er omfattet af tavshedspligten. Denne skærpede tavshedspligt går desuden videre end den tavshedspligt, der i medfør af § 27, stk. 1, i forvaltningsloven påhviler alle offentligt ansatte.

Tavshedspligten er i høj grad baseret på et ønske om at beskytte virksomhedernes kunder, det være sig privatpersoner eller erhvervskunder. Hertil kommer et ønske om af konkurrencemæssige grunde at beskytte virksomhedernes forretningsmæssige forhold. Herudover er Finanstilsynets tavshedspligt en afgørende betingelse for den tilsynsmæssige effektivitet. For at tilsynet kan få alle nødvendige oplysninger i en given sag, må virksomhederne og kunderne kunne nære tillid til, at Finanstilsynet ikke videregiver fortrolige oplysninger.

Med lovforslaget foreslås det at indsætte et nyt *nr. 44* i § 354, stk. 6, hvorefter Finanstilsynet kan videregive oplysninger til Center for Cybersikkerhed, under forudsætning af at oplysningerne er nødvendige for dem til opfyldelse af deres lovbestemte opgaver, i deres egenskab af CSIRT eller nationalt centralt kontaktpunkt.

Med bestemmelsen gennemføres NIS-direktivets artikel 10, stk. 1 og 2, hvorefter den kompetente myndighed samarbejder med den enhed, der håndterer hændelser, den såkaldte CSIRT. Det følger endvidere af direktivets artikel 1, nr. 5, at oplysninger der er fortrolige i henhold til EU-regler og nationale regler, kan udveksles med forbehold af artikel 346 i TEUF, 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.

Med henblik på at sikre et sådant samarbejde, foreslås det at Finanstilsynet kan videregive oplysninger til Center for Cybersikkerhed, i det omfang oplysningerne er nødvendige for, at Center for Cybersikkerhed kan varetage sine opgaver som nationalt centralt kontaktpunkt eller CSIRT, da det er forventningen, at Center for Cybersikkerhed, vil blive udpeget af Forsvarsministeriet som CSIRT og som nationalt centralt kontaktpunkt.

Med den foreslåede bestemmelse sikres det bl.a., at Finanstilsynet kan samarbejde med Center for Cybersikkerhed, herunder oplyse om de eventuelle hændelsesrapporteringer, som penge- eller realkreditinstitutter har foretaget til Finanstilsynet.

Det skal dog bemærkes, at i medfør af § 354, stk. 8, i lov om finansiel virksomhed vil fortroligheden følge oplysningerne, hvilket indebærer, at for så vidt angår de oplysninger, som Finanstilsynet videregiver til Center for Cybersikkerhed, så indebærer videregivelsen, at Center for Cybersikkerhed omfattes af den samme skærpede tavshedspligt som Finanstilsynet er underlagt efter § 354 i lov om finansiel virksomhed. Dette er i øvrigt i overensstemmelse med NIS-direktivet, hvoraf det følger af præambel nr. 41, at hvis der er tale om oplysninger, der 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 direktivet.

Endelig skal det bemærkes, at ved en eventuel videregivelse af personoplysninger vil de gældende regler vedrørende persondataloven tillige finde anvendelse, hvorfor behandling af persondata altid vil ske under iagttagelse af gældende lovgivning, herunder den kommende persondataforordning.

Til nr. 5

Forslaget til *§ 354 h* gennemfører NIS-direktivets artikel 14, stk. 6, hvorefter den kompetente myndighed kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Med den foreslåede bestemmelse kan Finanstilsynet efter høring af en virksomhed, der underretter Finanstilsynet og Center for Cybersikkerhed om en hændelse, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, orientere offentligheden om hændelsen, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangværende hændelse. Der vil være tale om de hændelser, som en virksomhed underetter om i medfør af de af Finanstilsynet nærmere fastsatte regler efter den foreslåede § 71, stk. 2, 2. pkt. Det forventes, at Finanstilsynet vil udnytte bemyndigelsen til at fastsætte nærmere regler om hændelsesrapportering i bekendtgørelse nr. 1026 af 30. juni 2016, om ledelse og styring af pengeinstitutter m.fl. Det er Finanstilsynet, der vurderer, hvornår en given hændelse er relevant for offentligheden.

Det foreslås med bestemmelsens 2. og 3. pkt., at offentliggørelsen ikke må indeholde fortrolige oplysninger om kundeforhold eller oplysninger omfattet af § 30 i lov om offentlighed i forvaltningen. Offentliggørelsen må ikke indeholde fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den

Europæiske Union, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse.

Det indebærer, at en offentliggørelse ikke må kunne indeholde oplysninger om kundeforhold eller oplysninger om virksomhedens interne forhold af væsentlig betydning for virksomheden, fx ikke-offentligt tilgængelige oplysninger om virksomhedens opbygning og indretning, dens økonomiske forhold og situation, dens kundemasse og dens samarbejdspartnere. Offentliggørelse af oplysninger om en hændelse indebærer ikke, at selve sagen bliver offentlig tilgængelig. Sagen vil således stadig være omfattet af Finanstilsynets tavshedspligt, og der vil heller ikke efter offentliggørelse være mulighed for at få aktindsigt i sagens dokumenter.

Af hensyn til samarbejdet mellem de finansielle tilsynsmyndigheder inden for EU/EØS-området foreslås det, at en offentliggørelse ikke må indeholde fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den Europæiske Union, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse. Offentliggørelse kan derfor kun ske, hvis den myndighed, der har givet de pågældende oplysninger til Finanstilsynet, giver deres udtrykkelige tilladelse hertil.

Forslaget om offentliggørelse af oplysninger om hændelser, som ovenfor beskrevet, er udarbejdet med baggrund i de anbefalinger, som fremgår af Justitsministeriets betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser m.v. I betænkningen anbefales det, at der inden indførelse af ordninger med systematisk offentliggørelse af oplysning om kontrolresultater, afgørelser m.v. på internettet i ikke-anonymiseret form foretages en vurdering af det konkrete behov for offentliggørelse, om offentliggørelse kan forventes konkret at være særligt indgribende for personen, om der er tungtvejende samfundsmæssige hensyn bag offentliggørelsesordningen, om offentliggørelse strider mod persondataloven og de almindelige regler om tavshedspligt, og om der af retssikkerhedsmæssige grunde er opstillet administrative regler for forvaltningsmyndighedens behandling af de enkelte sager.

Det er således Finanstilsynets vurdering om det er nødvendigt for at forebygge eller håndtere en igangværende hændelse at offentliggøre navnet på den berørte virksomhed, eller om det samme resultat kan nås med en anonymiseret offentliggørelse, som alene omfatter den konkrete hændelse. En offentliggørelse vil dog altid forudsætte, at den berørte virksomhed er blevet hørt herom. Det skal endvidere bemærkes, at en offentliggørelse endvidere vil ske under hensyntagen til bl.a. den kommende databeskyttelseslov og persondataforordningen.

Til § 20

Til nr. 1

Med den foreslåede ændring af fodnoten til lov om kapitalmarkeder indsættes en henvisning til, at der med denne lov foretages en gennemførelse af 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, idet lovforslaget implementerer de dele af direktivet i lov om kapitalmarkeder, der omfatter operatører af markedspladser og centrale modparter (CCP'er).

Til nr. 2

Forslaget til *§ 58 a, stk. 1 og 2,* gennemfører NIS-direktivets artikel 5, stk. 1-3 og stk. 5, hvorefter medlemsstaterne senest den 9. november 2018 identificerer operatører af væsentlige tjenester ud fra, at de tjenester der leveres er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af tjenesterne afhænger af net- og informationssystemer, og at en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesterne.

Med en hændelse forstås enhver begivenhed, der har en negativ indvirkning på sikkerheden i en operatørs net- og informationssystemer. Med sikkerhed i net- og informationssystemer forstås net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

Det følger endvidere af direktivets artikel 5, stk. 5, at listen over identificerede operatører af væsentlige tjenester tages op til revision mindst hvert andet år og ajourføres hvis relevant.

Med den foreslåede *§ 58 a, stk. 1*, skal Finanstilsynet mindst hvert andet år udpege de operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester.

Dermed skal Finanstilsynet mindst hvert andet år offentliggøre en liste over de operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester. Det indebærer at listen skal ajourføres løbende, og mindst hvert andet år. Det forventes at Finanstilsynet vil offentliggøre en liste første gang primo november 2018 i overensstemmelse med NIS-direktivets artikel 5, stk. 1.

Med den foreslåede *§ 58 a, stk. 2*, skal Finanstilsynet i forbindelse med udpegningen efter stk. 1, lægge vægt på tre kriterier.

Finanstilsynet skal for det første lægge vægt på, at de pågældende operatører af markedspladser og centrale modparter (CCP'er) udbyder en tjeneste, som er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

Finanstilsynet skal for det andet lægge vægt på, at de pågældende operatører af markedspladser og centrale modparters (CCP'ers) levering af tjenesten afhænger af net- og informationssystemer.

Endelig skal Finanstilsynet for det tredje lægge vægt på, at en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Med den foreslåede *§ 58 a, stk. 3, 1. pkt.*, kan Finanstilsynet fastsætte nærmere regler om identificeringen af operatører af væsentlige tjenester, herunder fastsætte nærmere krav om underretning af Finanstilsynet og Center for Cybersikkerhed ved en hændelse, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer.

I medfør af den foreslåede § 58 a, stk. 3, vil Finanstilsynet dermed kunne fastsætte nærmere regler for udpegningen efter stk. 1, herunder nærmere fastsætte hvilke kriterier der skal være opfyldt, for at en operatør af en markedsplads og en central modpart (CCP) udpeges som en operatør af væsentlige tjenester.

En operatør af en markedsplads kan enten være en operatør af et reguleret marked, en multilateral handelsfacilitet (MHF) eller en organiseret handels facilitet (OHF). En central modpart (CCP) er i § 3, nr. 11, defineret i artikel 2, nr. 1, i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre. Der findes ikke centrale modparter (CCP'er) i Danmark ved lovforslagets fremsættelse.

Bemyndigelsen i § 58 a, stk. 3, vil blive udnyttet ved en bekendtgørelse, som i medfør af det foreslåede stk. 3, endvidere vil indeholde regler om, hvornår en udpeget operatør af væsentlige tjenester skal underrette Finanstilsynet og Center for Cybersikkerhed om en hændelse, herunder hvilke oplysninger underretningen skal indeholde, og hvilke kriterier virksomheden skal lægge vægt på for at fastsætte konsekvenserne af en hændelse.

Med bestemmelsen gennemføres NIS-direktivets artikel 14, stk. 3, hvorefter en operatør af væsentlige tjenester hurtigst muligt skal foretage en underretning til den kompetente myndighed eller CSIRT, af hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som virksomheden leverer. En hændelse forstås som værende enhver begivenhed, der har en negativ indvirkning på sikkerheden i en virksomheds net- og informationssystemer. Med sikkerhed i net- og informationssystemer forstås net- og informationssystemernes 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.

Med den foreslåede § 58 a, stk. 3, gennemføres endvidere NIS-direktivets artikel 10, stk. 2, hvorefter medlemsstaterne skal sikre, at enten de kompetente myndigheder eller en CSIRT, som i Danmark forventes at blive Center for Cybersikkerhed, jf. nærmere herom under pkt. 3.2.3.3. i de almindelige bemærkninger, modtager underretning om hændelser, som har væsentlige konsekvenser for kontinuiteten af de tjenester, som de udpegede operatører af væsentlige tjenester leverer. I det omfang en CSIRT ikke modtager underretninger om hændelser, skal CSIRT'erne i stedet have oplysninger herom fra den kompetente myndighed.

Da Finanstilsynet som kompetent myndighed på det finansielle område fører tilsyn med de finansielle virksomheder, herunder virksomhedernes it-sikkerhed, foreslås det, at der sker underretninger om hændelser både til Finanstilsynet og Center for Cybersikkerhed som CSIRT, således at begge myndigheder hurtigst muligt orienteres om en hændelse, med henblik på bedre at kunne vurdere omfanget af en given hændelse.

En hændelse for en operatør af en markedsplads vil for eksempel kunne blive omfattet af underretningspligten, såfremt der er tale om en hændelse, der har negativ indvirkning på sikkerheden i virksomhedens net- og informationssystem, og hvor virksomheden kan blive udsat for et hacking angreb eller et svigt i it-systemet.

En anden hændelse der for eksempel vil kunne blive omfattet af underretningspligten, kan være en hændelse, der har væsentlige konsekvenser for kontinuiteten af driften af markedspladsen og den multilaterale handel med finansielle instrumenter, såsom en hændelse hvormed markedspladsens handelssystem svigter i en længere periode. Denne periode skal ses i forhold til, at der på en markedsplads bliver handlet finansielle instrumenter inden for sekunder, hvorfor en hændelse kan have haft væsentlige konsekvenser for driften af handelssystemet, hvis denne blot har været i nogle minutter.

For så vidt angår en central modpart (CCP), vil et svigt i den centrale modparts (CCP'ens) interne systemer, som hindrer fortsættelsen af korrekt sikkerhedsudveksling eller den clearede transaktions rettidige gennemførsel, bl.a. være at betragte som hændelser, som har væsentlige konsekvenser for kontinuiteten af de tjenester, som de udpegede operatører af væsentlige tjenester leverer.

Det fremgår af NIS-direktivets artikel 14, stk. 3, at en underretning skal indeholde oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. En underretning gør ikke den underrettende part til genstand for et øget ansvar.

En hændelses konsekvenser fastlægges navnlig ud fra 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. For at Finanstilsynet og Center for Cybersikkerhed, som national CSIRT, kan vurdere en hændelses konsekvenser, skal underretningerne indeholde oplysninger, der gør det muligt at fastslå hændelsens omfang og herunder eventuelle grænseoverskridende konsekvenser for hændelsen.

Det forventes derfor fastsat på bekendtgørelsesniveau i medfør af den foreslåede § 58 a, stk. 3, at en underretning skal indeholde oplysninger om antallet af medlemmer og udstedere på markedspladsen eller antallet og størrelsen af direkte og indirekte clearingmedlemmer hos den centrale modpart (CCP'en), der er berørt af hændelsen, oplysninger om hændelsens varighed og det geografiske område, der er berørt af hændelsen samt oplysninger om eventuelle grænseoverskridende konsekvenser af hændelsen.

I medfør af det foreslåede § 58 a, stk. 3, 2. pkt., vil Finanstilsynet ligeledes udarbejde en liste over tjenester, som

operatører af markedspladser og centrale modparter (CCP'er) leverer, der anses for at være væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter. Dette betyder, at en operatør af en markedsplads og en central modpart (CCP), der bliver udpeget som operatør af væsentlige tjenester, kan holde de væsentlige tjenester adskilt fra de ikke-væsentlige tjenester.

Til nr. 3

§ 225 i lov om kapitalmarkeder fastsætter i hvilke tilfælde og til hvem Finanstilsynet kan videregive fortrolige oplysninger, uanset Finanstilsynets særlige tavshedspligt som fremgår af § 224 i lov om kapitalmarkeder.

§ 224 indeholder hovedreglen om Finanstilsynets tavshedspligt og er en særbestemmelse om tavshedspligt, jf. offentlighedslovens § 35. Det indebærer, at der ikke vil være mulighed for adgang til aktindsigt efter offentlighedsloven i oplysninger hos Finanstilsynet, der er omfattet af tavshedspligten. Denne skærpede tavshedspligt går desuden videre end den tavshedspligt, der i medfør af § 27, stk. 1, i forvaltningsloven påhviler alle offentligt ansatte.

Tavshedspligten er i høj grad baseret på et ønske om at beskytte virksomhedernes kunder, det være sig privatpersoner eller erhvervskunder. Hertil kommer et ønske om af konkurrencemæssige grunde at beskytte virksomhedernes forretningsmæssige forhold. Herudover er Finanstilsynets tavshedspligt en afgørende betingelse for den tilsynsmæssige effektivitet. For at tilsynet kan få alle nødvendige oplysninger i en given sag, må virksomhederne og kunderne kunne nære tillid til, at Finanstilsynet ikke videregiver fortrolige oplysninger.

Med lovforslaget foreslås det at indsætte et nyt *nr. 17* i § 225, hvorefter Finanstilsynet kan videregive oplysninger til Center for Cybersikkerhed, under forudsætning af at oplysningerne er nødvendige for dem til opfyldelse af deres lovbestemte opgaver, i deres egenskab af CSIRT eller nationalt centralt kontaktpunkt.

Med bestemmelsen gennemføres NIS-direktivets artikel 10, stk. 1 og 2, hvorefter den kompetente myndighed samarbejder med den enhed, der håndterer hændelser, den såkaldte CSIRT. Det følger endvidere af direktivets artikel 1, nr. 5, at oplysninger der er fortrolige i henhold til EU-regler og nationale regler, kan udveksles med forbehold af artikel 346 i TEUF, 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.

Med henblik på at sikre et sådant samarbejde, foreslås det at Finanstilsynet kan videregive oplysninger til Center for Cybersikkerhed, i det omfang oplysningerne er nødvendige for, at Center for Cybersikkerhed kan varetage sine opgaver som nationalt centralt kontaktpunkt eller CSIRT. Det er forventningen, at Center for Cybersikkerhed, vil blive udpeget af Forsvarsministeriet som CSIRT og som det nationale centrale kontaktpunkt.

Med den foreslåede bestemmelse sikres det bl.a., at Finanstilsynet kan samarbejde med Center for Cybersikkerhed, herunder oplyse om de eventuelle indberetninger, som enten operatører af markedspladser eller centrale modparter (CCP'er) har foretaget til Finanstilsynet, jf. lovforslagets § 58 a, stk. 1.

Det skal dog bemærkes, at i medfør af § 229 i lov om kapitalmarkeder vil fortroligheden følge oplysningerne, hvilket indebærer, at for så vidt angår de oplysninger, som Finanstilsynet videregiver til Center for Cybersikkerhed, så indebærer videregivelsen, at Center for Cybersikkerhed omfattes af den samme skærpede tavshedspligt som Finanstilsynet er underlagt efter § 225 i lov om kapitalmarkeder. Dette er i øvrigt i overensstemmelse med NIS-direktivet, hvoraf det følger af præambel nr. 41, at hvis der er tale om oplysninger, der 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 direktivet.

Endelig skal det bemærkes, at ved en eventuel videregivelse af personoplysninger vil de gældende regler vedrørende persondataloven tillige finde anvendelse, hvorfor behandling af persondata altid vil ske under iagttagelse af gældende lovgivning, herunder den kommende persondataforordning.

Til nr. 4

Forslaget til *§ 236 a* gennemfører NIS-direktivets artikel 14, stk. 6, hvorefter den kompetente myndighed kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendig for at forebygge en hændelse eller håndtere en igangværende hændelse.

Med den foreslåede bestemmelse kan Finanstilsynet efter høring af en operatør af en markedsplads eller centrale modpart (CCP), der underretter Finanstilsynet og Center for Cybersikkerhed om en hændelse, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, orientere offentligheden om hændelsen, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangværende hændelse. Der vil være tale om de hændelser, som en virksomhed underetter om i medfør af de af Finanstilsynet nærmere fastsatte regler efter den foreslåede § 58 a, stk. 3 i lov om kapitalmarkeder. Det forventes, at Finanstilsynet vil udnytte bemyndigelsen til i en ny bekendtgørelse at fastsætte nærmere regler om hændelsesrapportering. Det er Finanstilsynet, der vurderer, hvornår en given hændelse er relevant for offentligheden.

Det foreslås med bestemmelsens 2. og 3. pkt., at offentliggørelsen ikke må indeholde fortrolige oplysninger om kundeforhold eller oplysninger omfattet af § 30 i lov om offentlighed i forvaltningen. Offentliggørelsen må ikke indeholde fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den Europæiske Union, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse.

Det indebærer, at en offentliggørelse ikke må indeholde oplysninger om kundeforhold eller oplysninger om virksomhedens interne forhold af væsentlig betydning for virksomheden, fx ikke-offentligt tilgængelige oplysninger om virksomhedens opbygning og indretning, dens økonomiske forhold og situation, dens kundemasse og dens samarbejdspartnere. Offentliggørelse af oplysninger om en hændelse indebærer ikke, at selve sagen bliver offentlig tilgængelig. Sagen vil således stadig være omfattet af Finanstilsynets tavshedspligt, og der vil heller ikke efter offentliggørelse være mulighed for at få aktindsigt i sagens dokumenter.

Af hensyn til samarbejdet mellem de finansielle tilsynsmyndigheder inden for EU/EØS-området foreslås det, at en offentliggørelse ikke må indeholde fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den Europæiske Union, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse. Offentliggørelse kan derfor kun ske, hvis den myndighed, der har givet de pågældende oplysninger til Finanstilsynet, giver deres udtrykkelige tilladelse hertil.

Forslaget om offentliggørelse af oplysninger om hændelser, som ovenfor beskrevet, er udarbejdet med baggrund i de anbefalinger, som fremgår af Justitsministeriets betænkning nr. 1516/2010 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser m.v. I betænkningen anbefales det, at der inden indførelse af ordninger med systematisk offentliggørelse af oplysning om kontrolresultater, afgørelser m.v. på internettet i ikke-anonymiseret form foretages en vurdering af det konkrete behov for offentliggørelse, om offentliggørelse kan forventes konkret at være særligt indgribende for personen, om der er tungtvejende samfundsmæssige hensyn bag offentliggørelsesordningen, om offentliggørelse strider mod persondataloven og de almindelige regler om tavshedspligt, og om der af retssikkerhedsmæssige grunde er opstillet administrative regler for forvaltningsmyndighedens behandling af de enkelte sager.

Det er således Finanstilsynets vurdering om det er nødvendigt for at forebygge eller håndtere en igangværende hændelse at offentliggøre navnet på den berørte virksomhed, eller om det samme resultat kan nås med en anonymiseret offentliggørelse, som alene omfatter den konkrete hændelse.

En offentliggørelse vil dog altid forudsætte, at den berørte virksomhed er blevet hørt herom. Det skal endvidere bemærkes, at en offentliggørelse endvidere vil ske under hensyntagen til bl.a. den kommende databeskyttelseslov og persondataforordningen.

Til § 21

Med § 21 fastlægges lovens territoriale gyldighed.

Det foreslås med *stk. 1*, at loven ikke skal gælde for Færøerne og Grønland.

Det foreslås imidlertid med *stk. 2*, at lovens §§ 19 og 20 kan sættes helt eller delvis i kraft for Færøerne og Grønland ved kongelig anordning med de ændringer, som de færøske og grønlandske forhold tilsiger.

§§ 19-20 vedrører ændringer til lov om finansiel virksomhed og lov om kapitalmarkeder, som gennemfører NIS-direktivet. Disse ændringer skal kunne sættes i kraft for Færøerne og Grønland med de ændringer, som de færøske og grønlandske forhold tilsiger.

Det foreslås endvidere, bestemmelserne kan sættes i kraft på forskellige tidspunkter.

Bilag

Lovforslag sammenholdt med gældende ret

Gældende lov

Fodnoten. Loven indeholder bestemmelser, der gennemfører dele af Rådets fjerde direktiv 78/660/EØF af 25. juli 1978 (4. selskabsdirektiv), EF-Tidende 1978, nr. L 222, side 11, dele af Rådets syvende direktiv 83/349/EØF af 13. juni 1983 (7. selskabsdirektiv), EF-Tidende 1983, nr. L 193, side 1, dele af Rådets ottende direktiv 84/253/EØF af 10. april 1984 (8. selskabsdirektiv), EF-Tidende 1984, nr. L 126, side 20, Rådets direktiv 86/635/EØF af 8. december 1986 (bankregnskabsdirektivet), EF-Tidende 1986, nr. L 372, side 1, Rådets direktiv 89/117/EØF af 13. februar 1989 (offentliggørelse af årsregnskabsdokumenter for filialer fra ikkemedlemslande), EF-Tidende 1989, nr. L 44, side 40, Rådets direktiv 91/674/EØF af 19. december 1991 (forsikringsregnskabsdirektivet), EF-Tidende 1991, nr. L 374, side 7, Europa-Parlamentets og Rådets direktiv 95/26/EF af 29. juni 1995 (BCCI-direktivet), EF-Tidende 1995, nr. L 168, side 7, dele af Europa-Parlamentets og Rådets direktiv 2000/26/EF af 16. maj 2000 (4. motorkøretøjsforsikringsdirektiv), EF-Tidende 2000, nr. L 181, side 65, Europa-Parlamentets og Rådets direktiv 2000/64/EF af 7. november 2000 (udveksling af oplysninger), EF-Tidende 2000, nr. L 290, side 27, Europa-Parlamentets og Rådets direktiv 2001/24/EF af 4. april 2001 (likvidationsdirektivet for kreditinstitutter), EF-Tidende 2001, nr. L 125, side 15, Europa-Parlamentets og Rådets direktiv 2002/13/EF af 5. marts 2002 (solvens I-direktivet), EF-Tidende 2002, nr. L 77, side 17, Europa-Parlamentets og Rådets direktiv 2002/87/EF af 16. december 2002 (konglomeratdirektivet), EU-Tidende 2003, nr. L 35, side 1, dele af Europa-Parlamentets og Rådets direktiv 2002/92/EF af 9. december 2002 (direktiv om forsikringsformidling), EF-Tiden-

Lovforslaget

§ 19

I lov om finansiel virksomhed jf. lovbekendtgørelse nr. 1140 af 26. september 2017, som bl.a. ændret ved § 1 i lov nr. 667 af 8. juni 2017, § 1 i lov nr. 1547 af 19. december 2017 og senest ved § 34 i lov nr. 1555 af 19. december 2017 foretages følgende ændringer:

1. I *fodnoten* til lovens titel ændres »og dele af Europa-Parlamentets og Rådets direktiv 2015/849/EU af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (4. hvidvaskdirektiv), EU-Tidende 2015, nr. L 141, side 73« til: » dele af Europa-Parlamentets og Rådets direktiv 2015/849/EU af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (4. hvidvaskdirektiv), EU-Tidende 2015, nr. L 141, side 73, og dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 (NIS-direktivet), EU-Tidende 2016, nr. L 194, side 1«.

de 2003, nr. L 9, side 3, dele af Europa-Parlamentets og Rådets direktiv 2005/14/EF af 11. maj 2005 (5. motorkøretøjsforsikringsdirektiv), EU-Tidende 2005, nr. L 149, side 14, dele af Europa-Parlamentets og Rådets direktiv 2006/31/EF af 5. april 2006 om ændring af direktiv 2004/39/EF om markeder for finansielle instrumenter, for så vidt angår visse frister (udsættelsesdirektivet), EU-Tidende 2006, nr. L 114, side 60, Europa-Parlamentets og Rådets direktiv 2007/44/EF af 5. september 2007 om ændring af Rådets direktiv 92/49/EØF og direktiv 2002/83/EF, 2004/39/EF, 2005/68/EF og 2006/48/EF, hvad angår procedurereglerne og kriterierne for tilsynsmæssig vurdering af erhvervelser og forøgelse af kapitalandele i den finansielle sektor (kapitalandelsdirektivet), EU-Tidende 2007, nr. L 247, side 1, dele af Europa-Parlamentets og Rådets direktiv 2007/64/EF af 13. november 2007 om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF (betalingstjenestedirektivet), EU-Tidende 2007, nr. L 319, side 1, dele af Europa-Parlamentets og Rådets direktiv 2009/65/EF af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer (investeringsinstitutter) (UCITS-direktivet), EU-Tidende 2009, nr. L 302, side 32, dele af Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II), EU-Tidende 2009, nr. L 335, side 1, Kommissionens direktiv 2010/43/EU af 1. juli 2010 om gennemførelse af Europa-Parlamentets og Rådets direktiv 2009/65/EF for så vidt angår organisatoriske krav, interessekonflikter, god forretningsskik, risikostyring og indholdet af aftalen mellem en depositar og et administrationsselskab, EU-Tidende 2010, nr. L 176, side 42, dele af Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde og om ændring af direktiv 2003/41/EF og 2009/65/EF samt forordning (EF) nr. 1060/2009 og (EU) nr. 1095/2010, EU-Tidende 2011, nr. L 174, side 1, Europa-Parlamentets og Rådets direktiv 2011/89/EU af 16. november 2011 om ændring af direktiv 98/78/EF, 2002/87/EF, 2006/48/EF og 2009/138/EF for så vidt angår det supplerende tilsyn med finansielle enheder i et finansielt konglomerat,

EU-Tidende 2011, nr. L 326, side 113, dele af Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 (CRD IV), EU-Tidende 2013, nr. L 176, side 338, Europa-Parlamentets og Rådets direktiv 2013/58/EU af 11. december 2013 om ændring af direktiv 2009/138/EF (Solvens II) for så vidt angår datoerne for dets gennemførelse og anvendelse og datoen for ophævelse af visse direktiver (Solvens I), EU-Tidende 2013, nr. L 341, side 1, dele af Europa-Parlamentets og Rådets direktiv 2014/17/EU af 4. februar 2014 om forbrugerkreditaftaler i forbindelse med fast ejendom til beboelse og om ændring af direktiv 2008/48/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 (boligkreditdirektivet), EU-Tidende 2014, nr. L 60, side 34, dele af Europa-Parlamentets og Rådets direktiv 2014/51/EU af 16. april 2014 om ændring af direktiv 2003/71/EF og 2009/138/EF samt forordning (EF) nr. 1060/2009, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 for så vidt angår de beføjelser, der er tillagt den europæiske tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger) og den europæiske tilsynsmyndighed (Den Europæiske Værdipapirtilsynsmyndighed), EU-Tidende 2014, nr. L 153, side 1, dele af Europa-Parlamentets og Rådets direktiv 2014/49/EU af 16. april 2014 om indskudsgarantiordninger (DGSD), EU-Tidende 2014, nr. L 173, side 149, dele af Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter (BRRD), EU-Tidende 2014, nr. L 173, side 190, dele af Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter (MiFID II), EU-Tidende 2014, nr. L 173, side 349, dele af Europa-Parlamentets og Rådets direktiv 2014/91/EU af 23. juli 2014 om ændring af direktiv 2009/65/EF om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer (investeringsinstitutter) for så vidt angår depositarfunktioner, aflønningspolitik og sanktioner (UCITS V-direktivet), EU-Tidende 2014, nr. L 257, side 186, og dele af Europa-Parlamentets og Rådets direktiv 2015/849/EU af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012

og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (4. hvidvaskdirektiv), EU-Tidende 2015, nr. L 141, side 73. I loven er der endvidere medtaget visse bestemmelser fra Kommissionens forordning (EU) nr. 584/2010 af 1. juli 2010 om gennemførelse af Europa-Parlamentets og Rådets direktiv 2009/65/EF for så vidt angår form og indhold af standardmodellen til anmeldelsesskrivelse og erklæring om investeringsinstituttet, brug af elektronisk kommunikation mellem kompetente myndigheder i forbindelse med anmeldelser og procedurer ved kontroller og undersøgelser på stedet samt udveksling af oplysninger mellem kompetente myndigheder, EU-Tidende 2010, nr. L 176, side 16, Europa-Parlamentets og Rådets forordning (EU) nr. 1092/2010 af 24. november 2010 om makrotilsyn på EU-plan med det finansielle system og om oprettelse af et europæisk udvalg for systemiske risici, EU-Tidende 2010, nr. L 331, side 1, Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF, EU-Tidende 2010, nr. L 331, side 12, Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF, EU-Tidende 2010, nr. L 331, side 48, Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF, EU-Tidende 2010, nr. L 331, side 84, Europa-Parlamentets og Rådets forordning (EU) nr. 346/2013 af 17. april 2013 om europæiske sociale iværksætterfonde, EU-Tidende 2013, nr. L 115, side 18, Europa-Parlamentets og Rådets forordning (EU) nr. 345/2013 af 17. april 2013 om europæiske venturekapitalfonde, EU-Tidende 2013, nr. L 115, side 1, Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 (CRR), EU-Tidende 2013,

nr. L 176, side 1, Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter (MiFIR), EU-Tidende 2014, nr. L 173, side 84, og Europa-Parlamentets og Rådets forordning (EU) nr. 1286/2014 af 26. november 2014 om dokumenter med central information om sammensatte og forsikringsbaserede investeringsprodukter til detailinvestorer (PRIIP'er), EU-Tidende 2014, nr. L 352, side 1. Ifølge artikel 288 i EUF-traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af disse bestemmelser i loven er således udelukkende begrundet i praktiske hensyn og berører ikke forordningernes umiddelbare gyldighed i Danmark.

§ 71. - - -

Stk. 2. Et gruppe 1-forsikringsselskab skal som led i selskabets virksomhedsstyring, jf. stk. 1, identificere selskabets nøglepersoner.

Stk. 3-4. - - -

2. I *§ 71, stk. 2,* indsættes som *2. pkt.*:

»Finanstilsynet kan desuden fastsætte nærmere regler om hændelsesrapportering for de virksomheder, der udpeges som operatører af væsentlige tjenester i medfør af § 307 a, herunder om at Finanstilsynet og Center for Cybersikkerhed underrettes ved en hændelse, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer.«

3. Efter afsnit VIII indsættes:

»Afsnit VIII a
Kapitel 18 a
Identifikation af operatører af væsentlige tjenester

§ 307 a. Finanstilsynet udpeger mindst hvert andet år de penge- og realkreditinstitutter, der er operatører af væsentlige tjenester.

Stk. 2. Finanstilsynet skal i forbindelse med udpegningen efter stk. 1, lægge vægt på, at

1) de tjenester, der leveres, er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,

2) leveringen af tjenesten afhænger af net- og informationssystemer, og

3) en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Stk. 3. Finanstilsynet kan fastsætte nærmere regler om udpegning af operatører af væsentlige tje-

nester og de kriterier Finanstilsynet kan lægge vægt på efter stk. 1 og 2. Finanstilsynet udarbejder en liste over tjenester, jf. stk. 2, nr. 1.«

§ 354. - - -
Stk. 1-5. - - -
Stk. 6. Bestemmelsen i stk. 1 er ikke til hinder for, at fortrolige oplysninger videregives til:
Nr. 1-43) - - -

4. I *§ 354, stk. 6,* indsættes som *nr. 44*:»
44) Center for Cybersikkerhed under forudsætning af at oplysningerne er nødvendige for centeret til at opfylde deres lovbestemte opgaver som nationalt centralt kontaktpunkt eller CSIRT.«

5. Efter § 354 g indsættes:

»§ 354 h. Finanstilsynet kan efter høring af den virksomhed, der underretter Finanstilsynet og Center for Cybersikkerhed om en hændelse, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, orientere offentligheden om hændelsen, hvis offentlighedens kendskab hertil er nødvendig for at forebygge eller håndtere en igangværende hændelse. Offentliggørelsen må ikke indeholde fortrolige oplysninger om kundeforhold eller oplysninger omfattet af § 30 i lov om offentlighed i forvaltningen. Offentliggørelsen må ikke indeholde fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den Europæiske Union, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse.«

§ 20

I lov om kapitalmarkeder, jf. lovbekendtgørelse nr. 12 af 8. januar 2018, foretages følgende ændringer:

Fodnoten. Loven indeholder bestemmelser, der gennemfører Europa-Parlamentets og Rådets direktiv 98/26/EF af 19. maj 1998, EF-Tidende 1998, nr. L 166, side 45, Europa-Parlamentets og Rådets direktiv 2001/34/EF af 28. maj 2001, EF-Tidende 2001, nr. L 184, side 1, Europa-Parlamentets og Rådets direktiv 2002/47/EF af 14. juni 2002, EF-Tidende 2002, nr. L 168, side 43, dele af Europa-Parla-

1. I *fodnoten* til lovens titel ændres »dele af Europa-Parlamentets og Rådets direktiv 2013/50/EU af 22. oktober 2013, EU-Tidende 2013, nr. L 294, side 13, og Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 349« til: »dele af Europa-Parlamentets og Rådets direktiv 2013/50/EU af 22. oktober 2013, EU-Tidende 2013, nr. L 294,

mentets og Rådets direktiv 2003/71/EF af 4. november 2003, EU-Tidende 2003, nr. L 345, side 64, dele af Europa-Parlamentets og Rådets direktiv 2004/25/EF af 21. april 2004, EU-Tidende 2004, nr. L 142, side 12, dele af Europa-Parlamentets og Rådets direktiv 2004/109/EF af 15. december 2004, EU-Tidende 2004, nr. L 390, side 38, dele af Kommissionens direktiv 2007/14/EF af 8. marts 2007 om gennemførelsesbestemmelser til visse bestemmelser i direktiv 2004/109/EF, EU-Tidende, nr. L 69, side 27, Europa-Parlamentets og Rådets direktiv 2009/44/EF af 6. maj 2009, EU-Tidende 2009, nr. L 146, side 37, dele af Europa-Parlamentets og Rådets direktiv 2010/73/EU af 24. november 2010, EU-Tidende 2010, nr. L 327, side 1, dele af Europa-Parlamentets og Rådets direktiv 2013/50/EU af 22. oktober 2013, EU-Tidende 2013, nr. L 294, side 13, og Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 349. I loven er der medtaget visse bestemmelser fra Kommissionens forordning nr. 1031/2010/EU af 12. november 2010, EU-Tidende 2010, nr. L 302, side 1, Europa-Parlamentets og Rådets forordning nr. 236/2012/EU af 14. marts 2012, EU-Tidende 2012, nr. L 86, side 1, dele af Europa-Parlamentets og Rådets forordning nr. 648/2012/EU af 4. juli 2012, EU-Tidende 2012, nr. L 201, side 1, Europa-Parlamentets og Rådets forordning nr. 600/2014 af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 84, Europa-Parlamentets og Rådets forordning nr. 909/2014 af 23. juli 2014, EU-Tidende, nr. L 257, side 1, Europa-Parlamentets og Rådets forordning (EU) nr. 596/2014 af 16. april 2014, EU-Tidende 2014, nr. L 173, side 1, og Europa-Parlamentets og Rådets forordning (EU) nr. 1011/2016 af 8. juni 2016, EU-Tidende 2016, nr. L 171, side 1. Ifølge artikel 288 i EUF-Traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af disse bestemmelser i loven er udelukkende begrundet i praktiske hensyn og berører ikke forordningernes umiddelbare gyldighed i Danmark.

side 13, Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 349, og dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016, EU-Tidende 2016, nr. L 194, side 1«.

2. Efter § 58 indsættes i afsnit IV:

»Identifikation af operatører af væsentlige tjenester

§ 58 a. Finanstilsynet udpeger mindst hvert andet år de operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester.

Stk. 2. Finanstilsynet skal i forbindelse med udpegningen efter stk. 1, lægge vægt på, at

1) de tjenester, der leveres, er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,

2) leveringen af tjenesten afhænger af net- og informationssystemer, og

3) en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Stk. 3. Finanstilsynet kan fastsætte nærmere regler om udpegning af operatører af væsentlige tjenester og de kriterier Finanstilsynet kan lægge vægt på efter stk. 1 og 2, herunder fastsætte nærmere regler om hændelsesrapportering, herunder om at Finanstilsynet og Center for Cybersikkerhed underrettes ved en hændelse, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer. Finanstilsynet udarbejder en liste over tjenester, jf. stk. 2, nr. 1.«

§ 225. § 224, stk. 1, er ikke til hinder for, at fortrolige oplysninger videregives til:

Nr. 1-16) - - -

Stk. 2. - - -

3. I *§ 225, stk. 1,* indsættes som *nr. 17*:

»17) Center for Cybersikkerhed under forudsætning af, at oplysningerne er nødvendige for centeret til opfyldelse af dets lovbestemte opgaver som nationalt centralt kontaktpunkt eller CSIRT.«

4. Efter § 236 indsættes før overskriften før § 237:

»§ 236 a. Finanstilsynet kan efter høring af en operatør af en markedsplads eller central modpart (CCP), der underretter Finanstilsynet og Center for Cybersikkerhed om en hændelse, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, orientere offentligheden om hændelsen, hvis offentlighedens kendskab hertil er nødvendig for at forebygge eller håndtere en igangværende hændelse. Offentliggørelsen må ikke indeholde fortrolige oplysninger om kundeforhold eller oplysninger omfattet af § 30 i lov om offentlighed i forvaltningen. Offentliggørelsen må ikke indeholde fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den Europæiske Union, medmindre de myndigheder,

der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse.«