LOV nr 436 af 08/05/2018 (Gældende) | **Udskriftsdato: 22. april 2020**

Ministerium: Erhvervsministeriet
Journalnummer: Erhvervsmin., Erhvervsstyrelsen, j.nr. 2018-2074

Senere ændringer til forskriften
LBK nr 457 af 24/04/2019
LBK nr 459 af 24/04/2019

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

VI MARGRETHE DEN ANDEN, af Guds Nåde Danmarks Dronning, gør vitterligt:

Folketinget har vedtaget og Vi ved Vort samtykke stadfæstet følgende lov:

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) Et 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 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 eller på et websted tilhørende en erhvervsdrivende, som anvender computingtjenester, 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 som 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 mål med risikoen. Udbyderen skal i den forbindelse inddrage følgende elementer:

1) Sikkerhed 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 af 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 oplyser offentligheden om dem, 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 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 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 og 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, f.eks. 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 § 45 i lov nr. 41 af 22. januar 2018 og senest ved § 2 i lov nr. 375 af 1. maj 2018, 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 dets lovbestemte opgaver som nationalt centralt kontaktpunkt eller som 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 som CSIRT.«

2. 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 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 delvis sættes i kraft for Færøerne og Grønland med de ændringer, som henholdsvis de færøske og de grønlandske forhold tilsiger. Bestemmelserne kan endvidere sættes i kraft på forskellige tidspunkter.

Givet på Amalienborg, den 8. maj 2018

Under Vor Kongelige Hånd og Segl

MARGRETHE R.

/ Brian Mikkelsen

[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.