2020/1 LSF 33 (Gældende)

Forslag til Lov om ændring af lov om net- og informationssikkerhed (Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester)

Ministerium: Forsvarsministeriet

Journalnummer: Forsvarsmin., j.nr.

Fremsat den 7. oktober 2020 af forsvarsministeren (Trine Bramsen)

Forslag

til

Lov om ændring af lov om net- og informationssikkerhed[1)]

(Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester)

§ 1

I lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed foretages følgende ændringer:

1. Lovens *titel* affattes således:

»Lov om sikkerhed i net og tjenester«.

2. *Fodnoten* til lovens titel affattes således:

»1) Loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning), EU-Tidende 2018, nr. L 321, side 36.«

3. *§ 1* affattes således:

»**§ 1.** Lovens formål er at fremme sikkerheden i net og tjenester.

Stk. 2. Henvisninger i loven og administrative forskrifter udstedt i medfør af loven til Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) med senere ændringer samt Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet) med senere ændring gælder som henvisninger til Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning) og skal læses efter sammenligningstabellen i direktivets bilag XIII.«

4. *§ 2* affattes således:

»**§ 2.** I denne lov forstås ved:

1) Elektronisk kommunikationsnet: Transmissionssystem, uanset om det bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres.
2) Elektronisk kommunikationstjeneste: Tjeneste, der helt eller delvis består i elektronisk overførsel af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter.
3) Offentligt tilgængelige elektroniske kommunikationsnet og -tjenester: Elektroniske kommunikationsnet og -tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.

4) Udbyder: Den, der med et kommercielt formål stiller produkter, elektroniske kommunikationsnet eller -tjenester til rådighed for andre. Begrebet omfatter ikke udbydere af NUIK-tjenester, jf. nr. 6.
5) Erhvervsmæssig udbyder: En udbyder, der med et kommercielt formål udbyder produkter, elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikke accessorisk del af virksomheden. Begrebet omfatter ikke udbydere af NUIK-tjenester, jf. nr. 6.
6) Udbyder af NUIK-tjeneste: En udbyder af en nummeruafhængig interpersonel kommunikationstjeneste i form af en tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer, hvem modtageren eller modtagerne skal være. Omfattet er ikke tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste. Tjenesten etablerer ikke forbindelse til offentligt tildelte nummerressourcer, dvs. et eller flere numre i nationale eller internationale nummerplaner, eller muliggør ikke kommunikation med et eller flere numre i nationale eller internationale nummerplaner.
7) Sikkerhed i net og tjenester: Net og tjenesters evne til på et givet fortrolighedsniveau at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af disse net og tjenester, lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net eller tjenester.
8) Sikkerhedshændelse: En begivenhed, der har en faktisk negativ indvirkning på sikkerheden i net og tjenester.«

5. I *overskriften* til kapitel 2 ændres »Informationssikkerhed« til: »Sikkerhed«.

6. *§ 3, stk. 1,* affattes således:

»Center for Cybersikkerhed fastsætter regler om minimumskrav til sikkerhed i net og tjenester for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til sikkerhed i net og tjenester og opretholdelse af et passende sikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.«

7. I *§ 3, stk. 2,* ændres »offentligt tilgængelige net og tjenester« til: »offentligt tilgængelige elektroniske kommunikationsnet og -tjenester«, og »informationssikkerheden« ændres til: »sikkerheden i net og tjenester«.

8. I *§ 3* indsættes efter stk. 2 som nyt stykke:

»Stk. 3. Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret. Centeret fastsætter nærmere regler herom.«

Stk. 3 bliver herefter stk. 4.

9. I *§ 3, stk. 3,* der bliver stk. 4, ændres »offentligt tilgængelige net og tjenester« til: »offentligt tilgængelige elektroniske kommunikationsnet og -tjenester«, og »informationssikkerheden i offentligt tilgængelige net og tjenester« ændres til: »sikkerheden i net og tjenester«.

10. I *§ 4, 1. pkt.,* indsættes efter »for udbydere«: »og udbydere af NUIK-tjenester«.

11. I *§ 4, nr. 1 og 2,* ændres »offentligt tilgængelige net og tjenesters« til: »offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters«.

12. *§ 4, nr. 3 og 4,* ophæves, og i stedet indsættes:

»3) Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters underretning af Center for Cybersikkerhed uden unødigt ophold om sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

4) Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters underretning af offentligheden ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

5) Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters informering af deres potentielt berørte brugere om mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe i tilfælde af en særlig og betydelig trussel om en sikkerhedshændelse i udbyderens net eller tjenester. Der kan endvidere stilles krav om, at de pågældende udbydere skal informere deres brugere om selve truslen.«

13. I *§ 5, stk. 2,* ændres »offentligt tilgængelige net og tjenester« til: »offentligt tilgængelige elektroniske kommunikationsnet og -tjenester«.

14. Efter § 5 indsættes i *kapitel 3:*

»§ 5 a. Center for Cybersikkerhed fastsætter regler om, at udbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.«

15. I *§ 6, stk. 1,* ændres »informationssikkerhed« til: »sikkerhed i net og tjenester«.

16. I *§ 6, stk. 2,* ændres »offentligt tilgængelige net« til: »offentligt tilgængelige elektroniske kommunikationsnet«.

17. I *§ 9, stk. 2,* ændres »udbydere« til: »udbydere og udbydere af NUIK-tjenester«, og »informationssikkerhed« ændres til: »sikkerhed i net og tjenester«.

18. I *§ 9, stk. 5,* ændres »udbydere« til: »udbydere og udbydere af NUIK-tjenester«.

19. I *§ 9, stk. 6, 1. pkt.,* og *stk. 7, 1. pkt.,* ændres »informationssikkerheden« til: »sikkerheden i net og tjenester«.

20. I *§ 10, stk. 1, nr. 1,* ændres »§ 3, stk. 2 og 3,« til »§ 3, stk. 2, 3 og 4,«, »§ 3, stk. 1 og 3,« ændres til: »§ 3, stk. 1, 3 og 4,«, og efter »§ 5, stk. 1, 2 og 3,« indsættes: »§ 5 a,«.

21. I *§ 10, stk. 2, nr. 1,* ændres »den udbyder« til: »den udbyder eller udbyder af NUIK-tjenester«.

22. I *§ 12, stk. 1 og 2,* ændres »udbydere« til: »udbydere og udbydere af NUIK-tjenester«, og »Det Europæiske Agentur for Net- og Informationssikkerhed« ændres til: »Den Europæiske Unions Agentur for Cybersikkerhed«.

23. I *§ 13* ændres »informationssikkerhed og beredskab på teleområdet« til: »sikkerhed i net og tjenester«.

24. I *§ 14, stk. 1, nr. 1,* ændres »§ 3, stk. 2 eller 3« til: »§ 3, stk. 2, 3 eller 4«.

25. I *§ 14, stk. 2,* ændres »§ 3, stk. 1 eller 3« til: »§ 3, stk. 1, 3 eller 4«, og efter »§ 5, stk. 1, 2 eller 3,« indsættes: »§ 5 a,«.

§ 2

Loven træder i kraft den 21. december 2020.

[1)] Loven gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning), EU-Tidende 2018, nr. L 321, side 36.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning
2. Lovforslagets baggrund
3. Lovforslagets hovedpunkter
   - 3.1. Indførelse af særskilt definition af udbydere af NUIK-tjenester
     - 3.1.1. Gældende ret
     - 3.1.2. Forsvarsministeriets overvejelser
     - 3.1.3. Den foreslåede ordning
   - 3.2. Sikkerhedskrav og underretningspligter
     - 3.2.1. Gældende ret
     - 3.2.2. Forsvarsministeriets overvejelser
     - 3.2.3. Den foreslåede ordning
   - 3.3. Påbud om konkrete foranstaltninger
     - 3.3.1. Gældende ret
     - 3.3.2. Forsvarsministeriets overvejelser
     - 3.3.3. Den foreslåede ordning
   - 3.4. Informering af brugere om beskyttelsesforanstaltninger m.v.
     - 3.4.1. Gældende ret
     - 3.4.2. Forsvarsministeriets overvejelser
     - 3.4.3. Den foreslåede ordning
   - 3.5. Uafbrudt transmission af offentlige advarsler
     - 3.5.1. Gældende ret
     - 3.5.2. Forsvarsministeriets overvejelser
     - 3.5.3. Den foreslåede ordning
4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige
5. Økonomiske og administrative konsekvenser for erhvervslivet m.v.
6. Administrative konsekvenser for borgerne
7. Klima- og miljømæssige konsekvenser
8. Forholdet til EU-retten
9. Hørte myndigheder og organisationer m.v.
10. Sammenfattende skema

1. Indledning

Europa-Parlamentet og Rådet har vedtaget direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (herefter EU's telekodeks). EU's telekodeks samler og reviderer fire centrale EU-direktiver på teleområdet.

Med EU's telekodeks forenkles EU-reguleringens nuværende struktur, så der skabes en mere sammenhængende regulering af elektroniske kommunikationsnet og -tjenester. Samtidig tages der med EU's telekodeks højde for den samfundsmæssige udvikling, hvor forbrugere og virksomheder i stadig stigende grad anvender digitale, internetbaserede tjenester frem for traditionelle teletjenester. På den baggrund indebærer revisionen også, at disse digitale, internetbaserede tjenester bliver omfattet af relevante dele af telereguleringen.

Klima-, Energi- og Forsyningsministeriet har det overordnede ressortansvar for EU's telekodeks. EU's

telekodeks indeholder dog også bestemmelser om sikkerheden i net og tjenester, der henhører under Forsvarsministeriets ressortansvar. Dette lovforslag har til formål at implementere EU's telekodeks på Forsvarsministeriets område.

EU's telekodeks regulerer – som noget nyt – internetbaserede kommunikationstjenester, der ikke anvender numre til dirigering af opkald, beskeder, mails eller lignende. Det vil oftest være tale-, video- eller beskedtjenester, herunder eksempelvis kommercielle alternativer til sms-beskeder, hvor to eller flere kan kommunikere sammen over internettet, men uden at anvende almindelige telefonnumre.

Lovforslaget indebærer, at der foreslås krav om sikkerhed i net og tjenester til denne nye kategori af udbydere af digitale, internetbaserede tjenester. Udbyderne betegnes i EU's telekodeks som udbydere af nummeruafhængige interpersonelle kommunikationstjenester (herefter udbydere af NUIK-tjenester).

Lovforslaget skal navnlig ses i sammenhæng med et samtidigt lovforslag fra Klima-, Energi- og Forsyningsministeriet, der implementerer EU's telekodeks, for så vidt angår bl.a. den sektorspecifikke konkurrenceregulering på teleområdet, administration af radiofrekvenser, administration af telefonnumre, særlige forbrugerrettigheder på teleområdet og forsyningspligt på kommunikationstjenester. Nærværende lovforslag har endvidere en vis sammenhæng med et andet, samtidigt lovforslag på Forsvarsministeriets område, der implementerer EU's telekodeks, for så vidt angår etablering af mobilbaseret varsling.

2. Baggrunden for lovforslaget

Forsvarets Efterretningstjenestes Center for Cybersikkerhed varetager Forsvarsministeriets myndighedsopgaver i relation til informationssikkerhed og beredskab på teleområdet.

I lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed er fastsat den overordnede ramme for de informationssikkerheds- og beredskabskrav, der stilles til udbydere af net og tjenester (herefter teleudbydere). Lovens bestemmelser om informationssikkerheds- og beredskabskrav er primært udformet som bemyndigelser, der er udmøntet administrativt af Center for Cybersikkerhed i fire bekendtgørelser. Loven indeholder desuden en række tilsyns- og håndhævelsesbestemmelser.

Visse dele af net- og informationssikkerhedsloven og de bekendtgørelser, der er udstedt med hjemmel i loven, bygger på EU-regulering. Lovgivningen implementerer således bestemmelser i Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), som senest ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009. De centrale bestemmelser i den henseende er rammedirektivets artikel 13 a og b, der stiller krav om, at der fastsættes sikkerhedskrav og underretningspligter for udbydere af offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester. Lovgivningen implementerer endvidere rammedirektivets artikel 5 om tilsyn og artikel 21 a om sanktioner.

Herudover implementerer lovgivningen artikel 23, 1. pkt., i Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009, der fastsætter krav til sikring af tilgængeligheden af offentligt tilgængelige telefonitjenester i tilfælde af netsvigt som følge af katastrofesituationer eller i force majeure-situationer.

Den nævnte EU-retlige regulering udstikker alene rammerne for medlemsstaternes krav til og tilsyn med informationssikkerhed og beredskab i telesektoren, og reguleringen pålægger medlemsstaterne at sikre, at teleudbydere træffer såkaldte passende foranstaltninger og foretager underretninger til tilsynsmyndigheden.

I december 2018 blev EU's telekodeks vedtaget af Europa-Parlamentet og Rådet. EU's telekodeks samler og reviderer de fire centrale EU-direktiver på teleområdet, herunder bl.a. rammedirektivet og

forsyningspligtdirektivet, der ikke er opdateret siden 2009. Formålet med revisionen er bl.a. at skabe de reguleringsmæssige rammer for udbredelsen af 5G-netværk samt tage højde for den samfundsmæssige udvikling, hvor forbrugere og virksomheder i stadig stigende grad anvender digitale, internetbaserede tjenester frem for traditionelle teletjenester. EU's telekodeks har derfor til formål at sikre, at disse digitale, internetbaserede tjenester også bliver omfattet af bl.a. passende informationssikkerhedskrav.

Som en væsentlig nyskabelse udvider EU's telekodeks således kredsen af forpligtede i relation til bl.a. sikkerheden i net og tjenester. Fremadrettet rettes kravene således ikke blot mod teleudbydere i traditionel forstand (udbydere af offentligt tilgængelige net og tjenester), men også mod udbydere af NUIK-tjenester.

Herudover videreføres de eksisterende informationssikkerhedskrav og underretningspligter med visse justeringer. Desuden indføres i EU's telekodeks en bestemmelse med inspiration fra Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om databeskyttelse inden for elektronisk kommunikation (e-databeskyttelsesdirektivet), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009, om udbyderes og udbydere af NUIK-tjenesters pligt til at informere brugere om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de kan træffe i tilfælde af en særlig og betydelig trussel om en sikkerhedshændelse. Det er hensigten, at den lignende bestemmelse i e-databeskyttelsesdirektivet ophæves i forbindelse med en forventet kommende revision af direktivet.

Vedtagelsen af EU's telekodeks indebærer, at der er behov for tilpasninger af den nuværende net- og informationssikkerhedslovgivning med henblik på implementering af direktivet. Direktivet skal være implementeret i dansk ret senest den 21. december 2020.

Forsvarsministeriet lægger vægt på, at implementering af EU's telekodeks sker i overensstemmelse med regeringens principper for implementering af erhvervsrettet EU-regulering, hvorefter den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen. Sikkerhedskrav og underretningspligter m.v. bør således nøje følge direktivets krav, så der ikke sker en overimplementering.

3. Lovforslagets hovedindhold

3.1. Indførelse af særskilt definition af udbydere af NUIK-tjenester

3.1.1. Gældende ret

Der er i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed fastsat regler om informationssikkerhedskrav og underretningspligter for de udbydere af offentligt tilgængelige net og tjenester, der er omfattet af rammedirektivets sikkerhedsbestemmelser i artikel 13 a og 13 b.

En udbyder er i net- og informationssikkerhedslovens § 2, nr. 4, defineret som den, der med et kommercielt formål stiller produkter, net eller tjenester til rådighed for andre. Offentligt tilgængelige net og tjenester er i lovens § 2, nr. 3, defineret som net og tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.

Ved en tjeneste forstås efter lovens § 2, nr. 2, en elektronisk kommunikationstjeneste, der helt eller delvis består i elektronisk overførsel af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter. Bestemmelsen hviler på rammedirektivets artikel 2, litra c. Definitionen er i øvrigt indholdsmæssigt identisk med definitionen af en elektronisk kommunikationstjeneste i § 2, nr. 7, i lov om elektroniske kommunikationsnet og -tjenester (teleloven), jf. lovbekendtgørelse nr. 128 af 7. februar 2014 med senere ændringer.

Elektroniske kommunikationstjenester mellem personer, der er baseret på en eksisterende internetforbindelse, og som ikke anvender numre fra den danske nummerplan, er ikke omfattet af den nuværende definition af en tjeneste i net- og informationssikkerhedslovens – eller telelovens – forstand.

3.1.2. Forsvarsministeriets overvejelser

Forpligtelserne i artikel 40 og 41 i EU's telekodeks vedrørende sikkerhedskrav og underretninger m.v. er rettet mod en bredere kreds af udbydere end de hidtidige regler i rammedirektivet. Det skyldes, at definitionen af en offentligt tilgængelig elektronisk kommunikationstjeneste i EU's telekodeks som noget nyt også omfatter nummeruafhængige, interpersonelle kommunikationstjenester, jf. artikel 2, nr. 4-7.

Som led i en implementering af EU's telekodeks på Forsvarsministeriets område vurderes der derfor at være behov for, at der i lovgivningen fastsættes sikkerhedskrav og underretningspligter m.v. over for disse udbydere af NUIK-tjenester.

3.1.3. Den foreslåede ordning

Det foreslås, at der i loven indføres en definition af udbydere af NUIK-tjenester, således at der kan fastsættes særskilte krav for disse udbydere. Dette skal ses i lyset af, at udbydere af NUIK-tjenester ikke på alle punkter kan sidestilles med de traditionelle teleudbydere, og at der derfor på visse punkter er behov for at kunne sondre mellem kravene til de forskellige typer af udbydere.

For at tydeliggøre sondringen mellem de nye udbydere af NUIK-tjenester og de traditionelle teleudbydere, som i forvejen var omfattet af loven, foreslås visse sproglige justeringer af de øvrige definitioner i lovens § 2, nr. 1-5. Disse justeringer har ingen selvstændig indholdsmæssig betydning.

3.2. Sikkerhedskrav og underretningspligter

3.2.1. Gældende ret

Det følger af net- og informationssikkerhedslovens § 3, stk. 1, at Center for Cybersikkerhed fastsætter regler om minimumskrav til informationssikkerhed for udbydere af offentligt tilgængelige net og tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til informationssikkerhed i offentligt tilgængelige net og tjenester og opretholdelse af et passende informationssikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Bestemmelsen implementerer rammedirektivets artikel 13 a, stk. 1 og 2.

Der er med hjemmel i bestemmelsen fastsat nærmere regler i bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester.

Udbydere af offentligt tilgængelige net og tjenester er desuden i medfør af net- og informationssikkerhedslovens § 4, nr. 3 og 4, der er udmøntet i bekendtgørelse nr. 1256 af 27. november 2019 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed, forpligtet til at foretage underretning af henholdsvis Center for Cybersikkerhed og offentligheden ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester.

Bestemmelserne i net- og informationssikkerhedslovens § 4, nr. 3 og 4, implementerer rammedirektivets artikel 13 a, stk. 3.

Det følger bl.a. af EU's telekodeks artikel 40, stk. 1, at medlemsstaterne skal sikre, at udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for på passende vis at styre risiciene for sikkerheden i net og tjenester. Under hensyn til teknologiens aktuelle stade skal disse foranstaltninger garantere et sikkerhedsniveau, der står i forhold til risikoen. Der skal navnlig træffes foranstaltninger, herunder kryptering, hvis det er relevant, for at forhindre og minimere virkningen af sikkerhedshændelser for brugerne og for andre net og tjenester.

Endvidere følger det bl.a. af EU's telekodeks artikel 40, stk. 2, at medlemsstaterne skal sikre, at udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester uden unødigt ophold underretter den kompetente myndighed om sikkerhedshændelser, der

har haft væsentlig indvirkning på driften af net eller tjenester. Med henblik på at fastlægge omfanget af en sikkerhedshændelses indvirkning tages navnlig følgende kriterier i betragtning, hvis de er til rådighed: a) antallet af brugere, der berøres af sikkerhedshændelsen, b) varigheden af sikkerhedshændelsen, c) den geografiske udbredelse med hensyn til det område, der er berørt af sikkerhedshændelsen, d) i hvilket omfang nettets eller tjenestens funktionsdygtighed påvirkes og e) omfanget af indvirkningen på økonomiske og samfundsmæssige aktiviteter.

3.2.2. Forsvarsministeriets overvejelser

Som led i en implementering af EU's telekodeks på Forsvarsministeriets område, finder Forsvarsministeriet, at der er behov for at tilpasse bestemmelserne i net- og informationssikkerhedslovens § 3, stk. 1, og § 4, nr. 3 og 4, på baggrund af ændringerne i EU's telekodeks artikel 40, stk. 1 og 2.

For så vidt angår sikkerhedskrav, implementerer § 3, stk. 1, i net- og informationssikkerhedsloven rammedirektivets artikel 13 a, stk. 1 og 2, om sikkerhedskrav. Disse bestemmelser er i EU's telekodeks sammenføjet og videreført i artikel 40, stk. 1, med visse justeringer. Justeringerne har primært sproglig karakter, men af mere indholdsmæssig betydning foretages der en tilføjelse vedrørende kryptering i artikel 40, stk. 1. Det følger af rammedirektivet i dag, at der bl.a. skal træffes passende og forholdsmæssige tekniske foranstaltninger, herunder navnlig foranstaltninger for at forhindre og minimere virkningen af sikkerhedshændelser. I EU's telekodeks præciseres det, at der navnlig skal træffes foranstaltninger, herunder kryptering, hvis det er relevant, for at forhindre og minimere virkningen af sikkerhedshændelser.

Der er allerede i dag i medfør af § 3, stk. 1, i net- og informationssikkerhedsloven hjemmel til at fastsætte krav om bl.a. passende tekniske foranstaltninger med henblik på risikostyring. Fremhævelsen af kryptering i EU's telekodeks som en mulig, relevant foranstaltning må efter Forsvarsministeriets opfattelse ses som et ønske om at fremme kryptering i relevant omfang, hvilket således bør være omfattet af hjemlen i § 3, stk. 1, i net- og informationssikkerhedsloven fremadrettet.

Som det fremgår af afsnit 3.1.2, indebærer udvidelsen af kredsen af pligtsubjekter, at der bl.a. skal fastsættes sikkerhedskrav over for udbydere af NUIK-tjenester. Det fremgår af direktivets betragtning 95, at eftersom udbyderne af NUIK-tjenester normalt ikke udøver egentlig kontrol over transmissionen af signaler via net, kan risikoen i forbindelse med disse tjenester i visse henseender anses for at være lavere end i forbindelse med traditionelle elektroniske kommunikationstjenester. Det er på den baggrund forudsat, at omfanget og styrken af sikkerhedskrav, der fastsættes over for udbydere af NUIK-tjenester, skal afspejle de faktiske sikkerhedsrisici forbundet med disse tjenester, og at der dermed kan være forskel på reguleringen af nummerafhængige og nummeruafhængige kommunikationstjenester.

Samtidig må der efter Forsvarsministeriets opfattelse ved fastsættelsen af sikkerhedskrav også lægges vægt på NUIK-tjenesternes stigende samfundsmæssige betydning. Hensigten med at udvide reguleringen til at omfatte denne type tjenester er således at styrke forbrugerbeskyttelsen ved at øge informationssikkerheden på tværs af tjenester, således at valget af tjeneste ikke er afgørende for, hvor sikker kommunikationen er.

Forsvarsministeriet finder på den baggrund, at hjemlen i § 3, stk. 1, i net- og informationssikkerhedsloven bør udvides til at omfatte udbydere af NUIK-tjenester, men at de krav, der fastsættes i medfør af bemyndigelsen overfor henholdsvis de traditionelle teleudbydere og udbyderne af NUIK-tjenester, bør afspejle forskellene i tjenesternes karakter. På den tekniske side vil det forhold, at udbyderne af NUIK-tjenester benytter internetudbydernes net, men uden at have kontrol over nettene, i praksis betyde, at sikkerhedskrav, der vedrører driften af disse net, ikke vil være relevante at rette mod udbydere af NUIK-tjenester. Udbyderne af NUIK-tjenester kan derimod have egen teknisk infrastruktur, herunder forbindelser til internetudbydernes net, som kan blive omfattet af sikkerhedskrav. I lighed med de traditionelle teleudbydere vil det i vidt omfang være relevant, at der overfor udbydere af NUIK-tjenester stilles

sikkerhedskrav af mere administrativ karakter, herunder eksempelvis processuelle og organisatoriske krav relateret til risikostyring.

For så vidt angår underretningspligt, er rammedirektivets artikel 13 a, stk. 3, i EU's telekodeks videreført i artikel 40, stk. 2, med visse justeringer.

Der er navnlig tale om, at artikel 40, stk. 2, i EU's telekodeks anvender begrebet "sikkerhedshændelser" som kriterium for underretningspligten, i modsætning til det hidtidige begreb "brud på sikkerheden eller tab af integritet" i rammedirektivets artikel 13 a, stk. 3. Der angives endvidere en række yderligere kriterier, som kan tages i betragtning ved vurderingen af omfanget af en sikkerhedshændelses indvirkning. Samtidig tilføjes et krav om, at underretning skal ske uden unødigt ophold.

Endelig betyder udvidelsen af kredsen af pligtsubjekter i EU's telekodeks, at udbydere af NUIK-tjenester også skal være omfattet af underretningspligterne i § 4, nr. 3 og 4, i net- og informationssikkerhedsloven.

3.2.3. Den foreslåede ordning

Det foreslås, at bestemmelserne i net- og informationssikkerhedslovens § 3, stk. 1, og § 4, nr. 3 og 4, videreføres med en række tilpasninger på baggrund af ændringerne i artikel 40, stk. 1 og 2, i EU's telekodeks.

Det foreslås, at bestemmelsen i lovens § 3, stk. 1, om krav til sikkerhed i net og tjenester fremadrettet også skal gælde for udbydere af NUIK-tjenester. Dermed bemyndiges Center for Cybersikkerhed til at fastsætte nærmere regler, som overfor udbydere af NUIK-tjenester stiller krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til sikkerheden i net og tjenester og opretholdelse af et passende sikkerhedsniveau. Det kan bl.a. omfatte krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Dette svarer i vidt omfang til ordningen for de traditionelle teleudbydere, om end der over for udbydere af NUIK-tjenester vil være hjemmel til, at der kan stilles andre og eventuelt færre krav end til de traditionelle teleudbydere, henset til, at tjenesterne ikke på alle punkter er sammenlignelige.

For så vidt angår underretningspligter, foreslås det, at lovens § 4, nr. 3 og 4, fremadrettet også skal gælde for udbydere af NUIK-tjenester. Derudover foreslås det, at der foretages visse tekniske justeringer af bestemmelserne, for så vidt angår kriterierne for underretningspligterne. Det foreslås således, at Center for Cybersikkerhed bemyndiges til at fastsætte nærmere regler om, at udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester skal underrette Center for Cybersikkerhed uden unødigt ophold om sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester. Det foreslås endvidere, at Center for Cybersikkerhed bemyndiges til at fastsætte nærmere regler om, at de pågældende udbydere skal underrette offentligheden om sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester. Som i dag indebærer dette, at udbyderne efter påbud skal underrette offentligheden, eller at Center for Cybersikkerhed kan foretage underretning af offentligheden, hvis det godtgøres, at dette er i offentlighedens interesse.

I overensstemmelse med artikel 2, nr. 42, i EU's telekodeks forstås en sikkerhedshændelse som en begivenhed, der har en faktisk negativ indvirkning på sikkerheden i elektroniske kommunikationsnet og -tjenester. Det foreslås i den forbindelse, at der indsættes en definition af en sikkerhedshændelse i lovens § 2.

3.3. Påbud om konkrete foranstaltninger

3.3.1. Gældende ret

Det følger af net- og informationssikkerhedslovens § 3, stk. 2, at Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige net og tjenester at inddrage nærmere angivne områder af deres

virksomhed og nærmere angivne trusler mod informationssikkerheden i deres risikostyringsprocesser efter stk. 1.

Det følger desuden af net- og informationssikkerhedslovens § 3, stk. 3, at såfremt det er af væsentlig samfundsmæssig betydning, kan Center for Cybersikkerhed påbyde udbydere af offentligt tilgængelige net og tjenester at træffe konkrete foranstaltninger med henblik på at sikre informationssikkerheden i offentligt tilgængelige net og tjenester. Bestemmelsen er nærmere udmøntet i bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester.

Det følger af EU's telekodeks artikel 41, stk. 1, at medlemsstaterne skal sikre, at de kompetente myndigheder har beføjelse til at pålægge udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester bindende instrukser, bl.a. om, hvilke foranstaltninger der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er blevet identificeret.

3.3.2. Forsvarsministeriets overvejelser

Som led i implementeringen af EU's telekodeks finder Forsvarsministeriet, at der er behov for at indsætte en ny bestemmelse i § 3 med henblik på implementering af artikel 41, stk. 1, i EU's telekodeks, som er ny.

Forpligtelsen i artikel 41, stk. 1, i EU's telekodeks vurderes på væsentlige punkter at adskille sig fra bestemmelserne i lovens § 3, stk. 2 og 3. Det skyldes – for så vidt angår den gældende § 3, stk. 2 – navnlig, at bestemmelsen ikke giver mulighed for at påbyde udbyderne at træffe konkrete foranstaltninger, men blot påbyde, at udbyderne skal inddrage bestemte områder af deres virksomhed og bestemte trusler i deres risikostyringsprocesser. For så vidt angår den gældende § 3, stk. 3, skyldes det navnlig, at det efter bestemmelsen er en betingelse for udstedelse af påbud om konkrete foranstaltninger, at dette er af væsentlig samfundsmæssig betydning, hvilket ikke er en betingelse i artikel 41, stk. 1, i EU's telekodeks. Derimod er der i artikel 41, stk. 1, krav om, at der i forhold til muligheden for at give bindende instrukser om forebyggende foranstaltninger skal være identificeret en betydelig trussel. Den gældende bestemmelse i § 3, stk. 3, har således et anderledes anvendelsesområde end artikel 41, stk. 1, i EU's telekodeks.

3.3.3. Den foreslåede ordning

Det foreslås, at der i § 3 indsættes en ny bestemmelse som stk. 3, hvorefter Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret. Centeret foreslås bemyndiget til at fastsætte nærmere regler herom.

Den foreslåede bestemmelse vil have til formål at implementere artikel 41, stk. 1, i EU's telekodeks.

Den foreslåede nye bestemmelse skal sikre, at der tages de nødvendige skridt til at håndtere en sikkerhedshændelse eller en betydelig trussel om en sikkerhedshændelse. Bestemmelsen vil således for det første kunne tages i anvendelse, hvis en sikkerhedshændelse er indtrådt, og hvis den pågældende udbyder samtidigt ikke af egen drift træffer de nødvendige foranstaltninger til at afhjælpe denne.

Bestemmelsen vil for det andet kunne tages i anvendelse, hvis der ikke på baggrund af bl.a. sikkerhedskravene fastsat i medfør af lovens § 3, stk. 1, herunder kravene til risikostyring, opnås en tilstrækkelig sikkerhed for, at det undgås, at en identificeret trussel, der vurderes som betydelig, fører til en sikkerhedshændelse.

3.4. Informering af brugere om beskyttelsesforanstaltninger m.v.

3.4.1. Gældende ret

Det følger af net- og informationssikkerhedslovens § 4, nr. 3 og 4, at udbydere af offentligt tilgængelige net og tjenester skal underrette Center for Cybersikkerhed, og i visse tilfælde offentligheden, ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester. Loven pålægger ikke udbydere at informere deres brugere om trusler om en sikkerhedshændelse eller mulige foranstaltninger, som brugerne kan træffe for at beskytte sig mod en trussel om en sikkerhedshændelse.

På Erhvervsministeriets område er det i medfør af telelovens § 8, stk. 4, i bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester fastsat, at udbydere af offentlige elektroniske kommunikationstjenester skal informere deres slutbrugere, hvis der er særlig risiko for brud på persondatasikkerheden, jf. bekendtgørelsens § 4. Hvis risikoen ligger uden for de foranstaltninger, der skal træffes af udbyderen efter bekendtgørelsen, skal udbyderen tillige informere slutbrugerne om, hvordan hændelsen i givet fald kan forebygges. Udbyderen skal herunder angive de omkostninger, der sandsynligvis vil være forbundet hermed.

Bekendtgørelsens § 4 implementerer artikel 4, stk. 2, i e-databeskyttelsesdirektivet. E-databeskyttelsesdirektivet supplerer de generelle EU-regler om beskyttelse af persondata og fastsætter særlige regler om databeskyttelse og privatlivsbeskyttelse på området for elektronisk kommunikation.

E-databeskyttelsesdirektivet er i øjeblikket under revision.

Det følger af EU's telekodeks artikel 40, stk. 3, at medlemsstaterne skal sikre, at udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, herunder NUIK-tjenester, jf. direktivets artikel 2, nr. 4-7, i tilfælde af en særlig og betydelig trussel om en sikkerhedshændelse i sådanne net og tjenester skal informere de af deres brugere, der potentielt er berørt af en sådan trussel, om eventuelle mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe. Hvis det er hensigtsmæssigt, skal udbyderne ligeledes underrette deres brugere om selve truslen.

3.4.2. Forsvarsministeriets overvejelser

Som led i implementeringen af EU's telekodeks finder Forsvarsministeriet, at der er behov for at indføre en ny bestemmelse, som skal gennemføre artikel 40, stk. 3, i EU's telekodeks.

EU's telekodeks artikel 40, stk. 3, er ny i forhold til de hidtidige regler i rammedirektivet, og den er indsat efter inspiration fra e-databeskyttelsesdirektivet. Forpligtelsen i EU's telekodeks har dog et andet fokus og anvendelsesområde end forpligtelsen i e-databeskyttelsesdirektivet, herunder som den kommer til udtryk i bekendtgørelsen om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

En central forskel er navnlig, at hvor forpligtelsen i EU's telekodeks vedrører information om beskyttelsesforanstaltninger i tilfælde af trusler om en sikkerhedshændelse, vedrører forpligtelsen i den eksisterende telelovgivning information om risiko for brud på persondatasikkerheden. Mens en sikkerhedshændelse er knyttet til tab af tilgængelighed, autenticitet, integritet og fortrolighed i net og tjenester, er brud på persondatasikkerheden knyttet til tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata i forbindelse med udbuddet af en offentlig elektronisk kommunikationstjeneste.

3.4.3. Den foreslåede ordning

Det foreslås, at der i § 4 indsættes et nyt nr. 5, hvor der indføres en forpligtelse for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester til at informere deres brugere om mulige beskyttelsesforanstaltninger m.v., som brugerne kan træffe i tilfælde af en særlig og betydelig trussel om en sikkerhedshændelse.

Det foreslås, at Center for Cybersikkerhed fastsætter nærmere regler herom. Ved fastsættelse af de nærmere regler vil der skulle tages højde for eventuelle retningslinjer fra EU.

Bestemmelsen vil have til formål at implementere artikel 40, stk. 3, i EU's telekodeks.

3.5. Uafbrudt transmission af offentlige advarsler

3.5.1. Gældende ret

Der er ikke i dag et mobilbaseret varslingssystem i Danmark, og der er derfor heller ikke pligt for teleudbydere til at sikre uafbrudt transmission af offentlige advarsler.

Udbydere af offentligt tilgængelige net og tjenester, herunder mobiloperatører, er imidlertid allerede i dag i medfør af bestemmelser i net- og informationssikkerhedslovens §§ 3 og 5 underlagt en række sikkerheds- og beredskabsforpligtelser med henblik på at sikre en robust teleinfrastruktur, herunder også i beredskabssituationer og andre ekstraordinære situationer.

Der kan således i medfør af lovens § 3, stk. 1, over for udbydere af offentligt tilgængelige net og tjenester stilles krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til informationssikkerhed i offentligt tilgængelige net og tjenester og opretholdelse af et passende informationssikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Det følger endvidere af lovens § 5, stk. 1, at udbydere efter nærmere regler herom skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Der kan med hjemmel i bestemmelsen i § 5, stk. 1, bl.a. stilles krav om, at udbyderne i deres beredskabsplanlægning skal tage stilling til fremskaffelse af det nødvendige reserveudstyr, adgang til den nødvendige eksterne hjælp, indgåelse af relevante serviceaftaler, samt behovet for medarbejdertilkaldeplaner i beredskabssituationer og i andre ekstraordinære situationer. Der kan endvidere stilles krav til sikring af redundans i nettene og om nødstrømsforsyning.

Det følger af EU's telekodeks artikel 108, 2. pkt., at medlemsstaterne skal sikre, at udbydere af talekommunikationstjenester træffer alle nødvendige foranstaltninger til at sikre uafbrudt adgang til beredskabstjenester og uafbrudt transmission af offentlige advarsler.

3.5.2. Forsvarsministeriets overvejelser

Som led i implementeringen af EU's telekodeks finder Forsvarsministeriet, at der er behov for at indføre en ny bestemmelse, som skal gennemføre den del af artikel 108, 2. pkt., i EU's telekodeks, der vedrører uafbrudt transmission af offentlige advarsler.

Det er i medfør af EU's telekodeks artikel 110 et krav, at udbydere af mobile nummerbaserede interpersonelle kommunikationstjenester (mobiloperatører) skal udsende offentlige advarsler, når offentlige varslingssystemer om overhængende eller truende alvorlige nødsituationer og katastrofer i et nærmere afgrænset område allerede er etableret.

Bestemmelsen vil blive implementeret ved en ændring af teleloven, da forpligtelsen har nær sammenhæng med eksisterende forpligtelser i teleloven i relation til bl.a. alarm- og beredskabsforhold. Der henvises til det nævnte lovforslag.

Det følger imidlertid også af EU's telekodeks artikel 108, 2. pkt., at medlemsstaterne bl.a. skal sikre, at udbydere af talekommunikationstjenester træffer alle nødvendige foranstaltninger til at sikre uafbrudt transmission af offentlige advarsler. Bestemmelsen forstås som vedrørende uafbrudt transmission af de offentlige advarsler, som er nævnt i direktivets artikel 110.

Forsvarsministeriet vurderer, at artikel 108, 2. pkt., mest hensigtsmæssigt kan implementeres i lov om net- og informationssikkerhed, da der er tale om sikkerhedsmæssige foranstaltninger.

3.5.3. Den foreslåede ordning

Det foreslås, at der som ny § 5 a indsættes en bestemmelse om, at Center for Cybersikkerhed kan fastsætte regler om, at udbydere, som i medfør af teleloven skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og naturkatastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.

Forpligtelsen til at udsende offentlige advarsler i medfør af teleloven forventes at påhvile de såkaldte mobiloperatører, som omfatter udbydere af elektroniske kommunikationstjenester i mobilnet og udbydere af mobilnet.

Den foreslåede bestemmelse i § 5 a indebærer, at mobiloperatørerne efter nærmere regler herom skal sikre, at transmissionen af offentlige advarsler til enhver tid kan opretholdes, herunder også i beredskabssituationer og andre ekstraordinære situationer. Henset til, at de offentlige advarsler har til formål at underrette befolkningen om overhængende eller truende alvorlige nødsituationer og katastrofer, er det særlig vigtigt at sikre pålideligheden af de systemer, der anvendes til transmission af offentlige advarsler.

Den foreslåede nye bestemmelse har til formål at sikre, at mobiloperatørerne – ud over hvad der allerede følger af bestemmelserne i net- og informationssikkerhedsloven – planlægger og træffer foranstaltninger for opretholdelsen af uafbrudt transmission af offentlige advarsler, herunder som led i en risikovurdering og beredskabsplanlægning sikrer udstyr og systemer, som anvendes i forbindelse med transmission af offentlige advarsler.

4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Lovforslaget indebærer, at Center for Cybersikkerhed i et vist omfang skal varetage yderligere opgaver. Det drejer sig navnlig om, at der med lovforslaget fastsættes sikkerhedskrav og underretningspligter m.v. for udbydere af NUIK-tjenester, og at Center for Cybersikkerhed, som er myndighed for informationssikkerhed og beredskab i telesektoren, vil skulle føre tilsyn med udbydernes overholdelse af reglerne. Det forventes, at der vil være visse administrative meromkostninger forbundet hermed, men at disse kan håndteres inden for eksisterende bevillingsmæssige rammer.

I det omfang stat, kommuner og regioner udbyder offentligt tilgængelige elektroniske kommunikationsnet og -tjenester eller NUIK-tjenester, vil de krav, der efter lovforslaget stilles til udbydere af disse net og tjenester, også omfatte stat, kommuner og regioner. Det vil kunne medføre økonomiske konsekvenser og implementeringskonsekvenser i samme omfang som for private udbydere.

Lovforslaget vurderes at være i overensstemmelse med principperne for digitaliseringsklar lovgivning. Det bemærkes navnlig i relation til den foreslåede ændring af lovens § 4, nr. 3, om udbydernes underretning af Center for Cybersikkerhed om sikkerhedshændelser, at den eksisterende, digitale selvbetjeningsløsning på virk.dk også fremadrettet forventes anvendt til underretninger efter den justerede bestemmelse. Dermed anvendes eksisterende offentlig it-infrastruktur til digital kommunikation mellem virksomhederne og Center for Cybersikkerhed.

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

Der foretages med lovforslaget en direktivnær implementering af EU's telekodeks. Implementeringen omfatter således alene de minimumsforpligtelser, der følger af direktivet.

Det vurderes samlet, at lovforslaget har øvrige efterlevelseskonsekvenser for erhvervslivet på væsentligt mindre end 10 mio. kr. Det vurderes endvidere samlet, at lovforslaget har administrative konsekvenser for erhvervslivet på mindre end 4 mio. kr.

5.1. Økonomiske og administrative konsekvenser for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

Med lovforslaget foretages en række tekniske justeringer af den eksisterende regulering af informations-

sikkerheden i telesektoren på baggrund af EU's telekodeks. For så vidt angår de traditionelle teleudbydere, der er omfattet af reguleringen i dag, foretages der med lovforslaget kun ganske få ændringer af eksisterende krav og ganske få tilføjelser af nye krav, som kan indebære merudgifter for disse udbydere. Udgifterne forventes at have et meget begrænset omfang.

Den foreslåede definition af sikkerhed i net og tjenester, der bl.a. omfatter sikring af autenticitet, vil kunne medføre behov for justering af eksisterende sikkerhedstiltag og derfor i begrænset omfang indebære økonomiske og administrative konsekvenser for de traditionelle teleudbydere. Der kan endvidere fastsættes justerede eller yderligere minimumskrav i medfør af lovens § 3, stk. 1, med henblik på gennemførelse af artikel 40, stk. 1, i EU's telekodeks, hvilket i et begrænset omfang kan have økonomiske og administrative konsekvenser. Herudover kan det medføre begrænsede økonomiske og administrative merudgifter, såfremt der i medfør af den foreslåede nye bestemmelse i § 3, stk. 3, gives påbud vedrørende nødvendige foranstaltninger for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret.

Efter den foreslåede § 5 a skal udbyderne efter nærmere regler herom træffe alle nødvendige foranstaltninger for at sikre uafbrudt transmission af offentlige advarsler. Det er besluttet, at staten afholder udgifterne forbundet med etablering og drift af et mobilbaseret offentligt varslingssystem. Staten vil således også afholde dokumenterede udgifter forbundet med krav i medfør af den foreslåede bestemmelse, som ikke allerede følger af de gældende §§ 3 og 5 i lov om net- og informationssikkerhed.

Det kan i et vist omfang have administrative konsekvenser for de traditionelle teleudbydere, at udbyderne som noget nyt efter regler, der udstedes i medfør af den foreslåede § 4, nr. 5, skal informere deres brugere om eventuelle beskyttelsesforanstaltninger i tilfælde af en særlig og betydelig trussel om en sikkerhedshændelse. Den foreslåede justering af underretningspligterne i lovens § 4, nr. 3 og 4, kan endvidere i begrænset omfang have administrative konsekvenser i det omfang, der skal foretages flere underretninger end hidtil, og henset til, at underretning skal ske uden unødigt ophold.

5.2. Økonomiske og administrative konsekvenser for udbydere af NUIK-tjenester

Lovforslaget indebærer, at der indføres sikkerhedskrav og underretningspligter m.v. for udbydere af NUIK-tjenester, der ikke tidligere har været omfattet af net- og informationssikkerhedsreguleringen.

Klima-, Energi- og Forsyningsministeriet anslår, at der vil være i størrelsesordenen 10-20 danske internetbaserede kommunikationstjenester, der vil kunne blive omfattet af definitionen.

Der kan således være økonomiske og administrative konsekvenser, herunder omstillingskonsekvenser, forbundet med disse udbyderes efterlevelse af de nye krav. De præcise omkostninger vil afhænge af udbydernes eksisterende sikkerhedsniveau og udviklingen i trusselsbilledet i samfundet, men det forventes, at omkostningerne vil være beskedne. Dette skal bl.a. ses i lyset af erfaringerne med de samme krav, der allerede i dag gælder for de traditionelle teleudbydere.

5.3. Agil erhvervsrettet regulering

Forsvarsministeriet vurderer, at visse af principperne for agil erhvervsrettet regulering er relevante for lovforslaget, og at lovforslaget er i overensstemmelse med principperne.

Der vurderes at være tale om enkel og formålsbestemt regulering. Der anvendes i lovforslaget i vidt omfang bemyndigelser for at sikre, at kravene løbende kan tilpasses. Der er dog ikke tale om meget specifikke detailkrav. Udbyderne vil således i ganske vidt omfang have metodefrihed med hensyn til, hvordan kravene nærmere gennemføres. Der kan bl.a. stilles krav om, at udbyderne overholder relevante og anerkendte internationale standarder, men uden at udbyderne pålægges at anvende en bestemt standard.

Der vurderes endvidere at være tale om teknologineutral regulering. Der stilles således ikke med lovforslaget direkte eller indirekte krav om anvendelse af bestemte teknologier.

I relation til den foreslåede ændring af lovens § 4, nr. 3, bemærkes det i øvrigt, at den eksisterende,

digitale selvbetjeningsløsning på virk.dk også fremadrettet forventes anvendt til udbydernes underretning af Center for Cybersikkerhed om sikkerhedshændelser. Dermed vil virksomhederne fortsat have én fælles portal til foretagelse af underretninger til forskellige myndigheder, herunder Center for Cybersikkerhed, hvilket vurderes at understøtte brugervenligheden.

6. Administrative konsekvenser for borgerne

Lovforslaget vurderes ikke at have administrative konsekvenser for borgerne.

7. Klima- og miljømæssige konsekvenser

Lovforslaget vurderes ikke at have klima- og miljømæssige konsekvenser.

8. Forholdet til EU-retten

Lovforslaget – og bekendtgørelser, der vil blive udstedt i medfør af de foreslåede bemyndigelser – gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU om oprettelse af en europæisk kodeks for elektronisk kommunikation.

Det bemærkes, at net- og informationssikkerhedsloven i dag gennemfører dele af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), som senest ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009, samt Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009.

EU's telekodeks sammenskriver, reviderer og ophæver de underliggende direktiver, herunder bl.a. rammedirektivet og forsyningspligtdirektivet. Det fastslås i EU's telekodeks, at forpligtelsen til at gennemføre direktivet i national ret kun bør omfatte de bestemmelser, hvori der er foretaget indholdsmæssige ændringer i forhold til de ophævede direktiver, jf. betragtning 325. Det følger endvidere af artikel 124, stk. 1, at medlemsstaterne vedtager og offentliggør senest den 21. december 2020 de love og administrative bestemmelser, der er nødvendige for at efterkomme dette direktiv. De meddeler straks Kommissionen teksten til disse love og bestemmelser. Medlemsstaterne anvender disse love og bestemmelser fra den 21. december 2020. Disse love og administrative bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De skal også indeholde oplysning om, at henvisninger i gældende love og administrative bestemmelser til de direktiver, der ophæves ved dette direktiv, gælder som henvisninger til dette direktiv. Medlemsstaterne fastsætter de nærmere regler for henvisningen og træffer bestemmelse om affattelsen af den nævnte oplysning.

På den baggrund foreslår Forsvarsministeriet, at der indsættes en bestemmelse om, at henvisninger i den gældende lov om net- og informationssikkerhed og i administrative bestemmelser udstedt i medfør af loven til de direktiver, der ophæves ved EU's telekodeks, gælder som henvisninger til EU's telekodeks.

Forsvarsministeriet lægger vægt på, at implementering af EU's telekodeks sker i overensstemmelse med regeringens principper for implementering af erhvervsrettet EU-regulering, hvorefter den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen.

9. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den 30. juli 2020 til den 27. august 2020 været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatrådet, Amnesty International, Bauer Media, Borch Teknik, Cibicom, Danmarks Radio, Dansk Beredskabskommunikation, Dansk Energi, Dansk Erhverv, Dansk Industri (DI), DANSK IT, Dansk Kabel TV, Danske Advokater, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DI Digi-

tal, Domstolsstyrelsen, Fibia, Forenede Danske Antenneanlæg, GLOBALCONNECT, Hi3G Denmark, HORESTA, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, Justitia, KL, Norlys, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rigsrevisionen, Rådet for Digital Sikkerhed, samtlige byretspræsidenter, TDC, TeleDCIS, Teleindustrien (TI), Telenor, Telia Company Danmark, TT-Netværket, TV 2 DTT og Waoo.

10. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/ Hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/ Hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen.	Ingen.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen.	Lovforslaget indebærer, at Center for Cybersikkerhed i et vist omfang skal varetage yderligere opgaver, herunder tilsyn med udbyderne af NUIK-tjenesters overholdelse af reglerne. Det forventes, at der vil være visse administrative meromkostninger forbundet hermed, men at disse kan håndteres inden for eksisterende bevillingsmæssige rammer.
Økonomiske konsekvenser for erhvervslivet	Ingen.	Det vurderes samlet, at lovforslaget har økonomiske konsekvenser for erhvervslivet på væsentligt mindre end 10 mio. kr.
Administrative konsekvenser for erhvervslivet	Ingen.	Det vurderes samlet, at lovforslaget har administrative konsekvenser for erhvervslivet på mindre end 4 mio. kr.
Administrative konsekvenser for borgerne	Ingen.	Ingen.
Klima- og miljømæssige konsekvenser	Ingen.	Ingen.
Forholdet til EU-retten	Lovforslaget – og bekendtgørelser, der vil blive udstedt i medfør af loven – gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU om oprettelse af en europæisk kodeks for elektronisk kommunikation.	
Er i strid med de principper for	Ja	Nej

implementering af erhvervsrettet EU-regulering/Går videre end minimumskrav i EU-regulering (sæt X)		X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Til nr. 1

Loven har i dag titlen "Lov om net- og informationssikkerhed".

Det foreslås, at lovens titel ændres fra "Lov om net- og informationssikkerhed" til "Lov om sikkerhed i net og tjenester". Forslaget er en konsekvens af forslaget om at anvende begrebet "sikkerhed i net og tjenester", som introduceres med EU's telekodeks, og som er defineret i den foreslåede § 2, nr. 7. Der henvises herom til bemærkningerne til lovforslagets § 1, nr. 4.

Til nr. 2

Det fremgår af den gældende fodnote til lov om net- og informationssikkerhed, at loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), EU-Tidende 2002, nr. L 108, side 33, som senest ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009, samt Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet), EU-Tidende 2002, nr. L 108, side 51, som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009.

EU's telekodeks ophæver og erstatter bl.a. rammedirektivet og forsyningspligtdirektivet, som på Forsvarsministeriets område er implementeret i den gældende net- og informationssikkerhedslov. Som konsekvens af ophævelsen af de to direktiver, foreslås fodnoten til loven ændret, således at fodnoten blot henviser til EU's telekodeks.

Med forslaget vil det fremgå af fodnoten til loven, at loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning), EU-Tidende 2018, nr. L 321, side 36.

Til nr. 3

Det fremgår af den gældende § 1, at lovens formål er at fremme net- og informationssikkerheden i samfundet.

Det følger af den foreslåede nyaffattelse af § 1, *stk. 1,* at lovens formål er at fremme sikkerheden i net og tjenester.

Det danske samfund har i de seneste år oplevet en rivende teknologisk udvikling i form af digitalisering. Digitaliseringen har i betydelig grad påvirket, hvordan borgere, virksomheder og det offentlige kommunikerer, og hvordan virksomheder og myndigheder organiseres og varetager deres opgaver. Digitaliseringen bliver stedse mere kompleks og har i de senere år været karakteriseret ved, at systemer og produkter i høj grad er online og indbyrdes forbundne.

Digitaliseringen forudsætter derfor en robust informations- og kommunikationsteknologisk infrastruktur (ikt-infrastruktur), som teleområdet er en væsentlig del af. En robust ikt-infrastruktur har dermed fået en helt central rolle i samfundets funktion, sammenhæng og værdiskabelse. Det er derfor af afgørende betyd-

ning for samfundet, at ikt-infrastrukturen er sikret, således at elektronisk kommunikation kan opretholdes, og at informationer kan udveksles fortroligt og uforvansket.

Formålet med loven er på den baggrund at medvirke til at sikre en robust ikt-infrastruktur ved at fremme sikkerheden i net og tjenester samt sikre, at elektronisk kommunikation kan finde sted i beredskabssituationer og i andre ekstraordinære situationer.

Sikkerhed i net og tjenester skal forstås som net og tjenesters evne til på et givet fortrolighedsniveau at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af disse net og tjenester, lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net eller tjenester. Der henvises herom til bemærkningerne til lovforslagets § 1, nr. 4.

Det følger af den foreslåede nyaffattelse af § 1, *stk. 2,* at henvisninger i loven og administrative forskrifter udstedt i medfør af loven til Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) med senere ændringer samt Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet) med senere ændring gælder som henvisninger til Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning) og skal læses efter sammenligningstabellen i direktivets bilag XIII.

Lovforslaget – og bekendtgørelser, der vil blive udstedt i medfør af de foreslåede bemyndigelser – gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU om oprettelse af en europæisk kodeks for elektronisk kommunikation.

Det bemærkes, at net- og informationssikkerhedsloven samt bekendtgørelser udstedt i medfør heraf i dag gennemfører dele af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) med senere ændringer samt Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet) med senere ændring.

EU's telekodeks sammenskriver, reviderer og ophæver de underliggende direktiver, herunder bl.a. rammedirektivet og forsyningspligtdirektivet. De bestemmelser i den gældende lov om net- og informationssikkerhed, som implementerer rammedirektivet og forsyningspligtdirektivet, og som ikke ændres med lovforslaget, vil med den foreslåede bestemmelse i § 1, stk. 2, fremadrettet implementere EU's telekodeks. Det drejer sig om den gældende § 5, stk. 1, og § 12, stk. 3.

Til nr. 4

Den gældende § 2 definerer i dag fem centrale begreber i loven. Definitionerne bygger på de tilsvarende definitioner i lov om elektroniske kommunikationsnet og -tjenester (teleloven), jf. lovbekendtgørelse nr. 128 af 7. februar 2014 med senere ændringer.

Det følger af den foreslåede nyaffattelse af lovens § 2, at der foretages en række sproglige ændringer af de fem nuværende definitioner i den gældende § 2, nr. 1-5. Der foreslås endvidere tre nye definitioner som § 2, nr. 6-8. De foreslåede ændringer af bestemmelsen skal ses i lyset af en række definitoriske ændringer i EU's telekodeks.

Efter den foreslåede § 2, nr. 1, defineres "elektronisk kommunikationsnet" som transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af

signaler, net, som anvendes til radio- og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres.

Definitionen af elektroniske kommunikationsnet foreslås justeret for at sikre overensstemmelse med definitionen af elektroniske kommunikationsnet i artikel 2, nr. 1, i EU's telekodeks. Forslaget er endvidere identisk med et forslag om at ændre den tilsvarende definition i teleloven, der indgår i et samtidigt lovforslag fra Klima-, Energi- og Forsyningsministeriet.

Det fremgår bl.a. af det samtidige lovforslag fra Klima-, Energi- og Forsyningsministeriet, at med den foreslåede justering vil definitionen omfatte alle transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet.

Definitionen vil således være identisk med den kommende definition af elektroniske kommunikationsnet i telelovens § 2, nr. 4, og bestemmelsen skal fortolkes i overensstemmelse med forarbejderne til den foreslåede bestemmelse i teleloven og relevant praksis i medfør af denne bestemmelse.

Efter den foreslåede § 2, *nr. 2,* defineres "elektronisk kommunikationstjeneste" som en tjeneste, der helt eller delvis består i elektronisk overførsel af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter.

Definitionen af en elektronisk kommunikationstjeneste svarer til den gældende definition i loven, og der foretages således kun en sproglig justering for at tydeliggøre sondringen mellem de traditionelle teletjenester, som er omfattet af den gældende lov, og de NUIK-tjenester, som bliver omfattet af loven i medfør af den foreslåede § 2, nr. 6, om udbydere af NUIK-tjenester.

Definitionen af en elektronisk kommunikationstjeneste er fortsat indholdsmæssigt identisk med definitionen af en elektronisk kommunikationstjeneste i telelovens § 2, nr. 7, og bestemmelsen skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Begrebet nettermineringspunkt skal forstås i overensstemmelse med definitionen heraf i telelovens § 2, nr. 6, hvorefter et nettermineringspunkt defineres som den fysiske eller logiske grænseflade i et elektronisk kommunikationsnet, der udgør en slutbrugers tilslutning til dette.

Efter den foreslåede § 2, *nr. 3,* defineres "offentligt tilgængelige elektroniske kommunikationsnet og -tjenester" som elektroniske kommunikationsnet og -tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere. Definitionen svarer til den gældende definition i loven, idet der blot foretages visse sproglige justeringer som konsekvens af ændrede formuleringer i de foreslåede § 2, nr. 1 og 2.

Definitionen svarer som hidtil til definitionen af såvel offentlige elektroniske kommunikationsnet i telelovens § 2, nr. 5, som offentlig elektronisk kommunikationstjeneste i telelovens § 2, nr. 8. Det bemærkes i den forbindelse, at det i et samtidigt lovforslag om ændring af teleloven fra Klima-, Energi- og Forsyningsministeriet foreslås at justere definitionen af offentlige elektroniske kommunikationsnet i telelovens § 2, nr. 5, således at denne er sprogligt identisk med den tilsvarende definition i EU's telekodeks. Det fremgår af Klima- Energi- og Forsyningsministeriets lovforslag, at der ikke med den foreslåede justering er tilsigtet en indholdsmæssig ændring af definitionen af offentlige elektroniske kommunikationsnet.

Den foreslåede § 2, nr. 3, skal fortolkes i overensstemmelse med forarbejderne til de nævnte bestemmelser i teleloven og relevant praksis i medfør heraf. Begrebet slutbruger skal forstås i overensstemmelse med definitionen heraf i telelovens § 2, nr. 3.

En "udbyder" defineres i den foreslåede § 2, *nr. 4,* som den, der med et kommercielt formål stiller produkter, elektroniske kommunikationsnet eller -tjenester til rådighed for andre. Definitionen er fortsat indholdsmæssigt identisk med den tilsvarende definition i telelovens § 2, nr. 1, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis. Der foreslås dog indsat en tydeliggørelse af, at begrebet ikke omfatter udbydere af NUIK-tjenester, jf. den foreslåede § 2, nr. 6.

Om indførelsen af en særskilt definition af udbydere af NUIK-tjenester henvises der i øvrigt til afsnit 3.1 i de almindelige bemærkninger.

En "erhvervsmæssig udbyder" defineres i den foreslåede § 2, *nr. 5,* som en udbyder, der med et kommercielt formål udbyder produkter, elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikke accessorisk del af virksomheden. Begrebet omfatter ikke udbydere af NUIK-tjenester, jf. den foreslåede nr. 6.

Om indførelsen af en særskilt definition af udbydere af NUIK-tjenester, henvises der i øvrigt til afsnit 3.1 i de almindelige bemærkninger.

Definitionen svarer til den gældende definition i loven, idet der blot foretages visse sproglige justeringer som konsekvens af ændrede formuleringer i de foreslåede § 2, nr. 1 og 2. Der foreslås endvidere indsat en tydeliggørelse af, at begrebet ikke omfatter udbydere af NUIK-tjenester, jf. den foreslåede § 2, nr. 6.

Definitionen er fortsat indholdsmæssigt identisk med den tilsvarende definition i telelovens § 2, nr. 2, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

I definitionerne af udbydere og erhvervsmæssige udbydere af elektroniske kommunikationsnet eller -tjenester benyttes – i overensstemmelse med de tilsvarende definitioner i teleloven – begrebet "produkter", som dækker over fysiske genstande, der ikke falder ind under definitionen af et elektronisk kommunikationsnet eller en elektronisk kommunikationstjeneste. Sådanne produkter kan eksempelvis være mobiltelefoner.

Det bemærkes i den forbindelse, at loven alene vedrører krav til sikkerhed i net og tjenester og beredskab i net og tjenester, hvorimod produkter ikke i øvrigt reguleres i loven.

En "udbyder af NUIK-tjeneste" defineres i den foreslåede § 2, *nr. 6,* som en udbyder af en nummeruafhængig interpersonel kommunikationstjeneste i form af en tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer, hvem modtageren eller modtagerne skal være. Omfattet er ikke tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste. Tjenesten etablerer ikke forbindelse til offentligt tildelte nummerressourcer, dvs. et eller flere numre i nationale eller internationale nummerplaner, eller muliggør ikke kommunikation med et eller flere numre i nationale eller internationale nummerplaner.

Den foreslåede definition er ny og implementerer artikel 2, nr. 7, i EU's telekodeks. Definitionen af en NUIK-tjeneste svarer indholdsmæssigt til den tilsvarende definition, der foreslås indsat i telelovens § 2, nr. 20, ved Klima-, Energi- og Forsyningsministeriets samtidige lovforslag om ændring af teleloven og andre love. Til forskel fra den foreslåede definition i teleloven, der angår en "nummeruafhængig, interpersonel kommunikationstjeneste", foreslås det i nærværende lov blot at anvende begrebet "udbyder af NUIK-tjeneste". Bestemmelsen skal fortolkes i overensstemmelse med forarbejderne til den foreslåede bestemmelse i teleloven og den relevante praksis, der måtte udvikle sig i medfør heraf.

Forslaget skal ses i lyset af, at det nu ophævede rammedirektiv og forsyningspligtdirektiv regulerede udbydere af elektroniske kommunikationstjenester, som nærmere defineret i teleloven og § 2, nr. 4, jf. § 2, nr. 2, i net- og informationssikkerhedsloven, herunder internetbaserede kommunikationstjenester, der anvender numre til dirigering (traditionelle udbydere af elektroniske kommunikationstjenester), hvorimod EU's teledirektiv også regulerer internetbaserede kommunikationstjenester, der ikke anvender numre til dirigering af opkald, beskeder, mails eller lignende.

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

I den foreslåede § 2, *nr. 7,* defineres "sikkerhed i net og tjenester" som net og tjenesters evne til på et givet fortrolighedsniveau at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten,

integriteten eller fortroligheden af disse net og tjenester, lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net eller tjenester.

Definitionen er ny og implementerer artikel 2, nr. 21, i EU's telekodeks.

Loven anvender i dag begrebet informationssikkerhed, hvilket forstås som sikring af tilgængelighed, fortrolighed og integritet i net og tjenester. Med definitionen af sikkerhed i net og tjenester udvides sikkerhedsområdet til – ud over tilgængelighed, fortrolighed og integritet – også at omfatte autenticitet. Autenticitet forstås i denne sammenhæng som det forhold, at data og informationssystemer m.v. er, hvad de foregiver at være. Begrebet handler således om ægthed eller originalitet.

Eftersom der er indholdsmæssig forskel på det hidtidige begreb "informationssikkerhed" og begrebet "sikkerhed i net og tjenester" som defineret i EU's telekodeks, foreslås det, at der generelt anvendes begrebet "sikkerhed i net og tjenester". Dette har bl.a. betydning for de sikkerhedsforpligtelser, der følger af loven, idet de fremadrettet vil omfatte både tilgængelighed, fortrolighed, integritet og autenticitet.

I den foreslåede § 2, *nr. 8,* defineres en "sikkerhedshændelse" som en begivenhed, der har en faktisk negativ indvirkning på sikkerheden i net og tjenester.

Definitionen er ny og implementerer artikel 2, nr. 42, i EU's telekodeks.

Begrebet "sikkerhedshændelse" erstatter begrebet "brud på informationssikkerheden", der indgår i underretningsforpligtelserne i lovens § 4, nr. 3 og 4.

En sikkerhedshændelse efter den foreslåede § 2, nr. 8, adskiller sig fra den type hændelse, der er omfattet af lovens § 8, stk. 1. Efter den gældende § 8, stk. 1, der ikke foreslås ændret, kan myndigheder og virksomheder underrette Center for Cybersikkerhed om hændelser, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale servicer. Med "hændelse" i lovens § 8, stk. 1, forstås således fortsat en sikkerhedshændelse som omfattet af lov om Center for Cybersikkerhed, og ikke en sikkerhedshændelse efter den foreslåede § 2, nr. 8.

Begrebet sikkerhedshændelse efter den foreslåede § 2, nr. 8, adskiller sig endvidere fra den type hændelse, der er omfattet af den gældende § 5, stk. 4. Efter den gældende § 5, stk. 4, der ikke foreslås ændret, kan Center for Cybersikkerhed i beredskabssituationer og i andre ekstraordinære situationer påbyde erhvervsmæssige udbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller en trussel, der i betydeligt omfang påvirker eller kan påvirke udbuddet af net eller tjenester negativt.

Bestemmelsen i lovens § 5, stk. 4, omfatter således også hændelser, der *kan* påvirke udbuddet af net eller tjenester negativt, hvorimod en sikkerhedshændelse efter den foreslåede § 2, nr. 8, forstås som en begivenhed, der har en faktisk negativ indvirkning på sikkerheden i net og tjenester.

Om underretninger om sikkerhedshændelser henvises der i øvrigt til afsnit 3.2 i de almindelige bemærkninger.

Til nr. 5

Overskriften til lovens gældende kapitel 2 er "Informationssikkerhed i net og tjenester". Det følger af den foreslåede ændring af overskriften, at denne bliver "Sikkerhed i net og tjenester".

Det foreslås således, at "informationssikkerhed" i overskriften til kapitel 2 ændres til "sikkerhed".

Forslaget er en konsekvens af forslaget om at anvende begrebet "sikkerhed i net og tjenester", som introduceres med EU's telekodeks, og som er defineret i den foreslåede § 2, nr. 7. Der henvises til bemærkningerne til lovforslagets § 1, nr. 4.

Til nr. 6

Det fremgår af den gældende § 3, stk. 1, at Center for Cybersikkerhed fastsætter regler om mini-

mumskrav til informationssikkerhed for udbydere af offentligt tilgængelige net og tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til informationssikkerhed i net og tjenester og opretholdelse af et passende informationssikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Bestemmelsen implementerer i dag rammedirektivets artikel 13 a, stk. 1 og 2.

Det følger af den foreslåede nyaffattelse af § 3, *stk. 1,* at Center for Cybersikkerhed fastsætter regler om minimumskrav til sikkerhed i net og tjenester for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til sikkerhed i net og tjenester og opretholdelse af et passende sikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Bestemmelsen justeres med henblik på implementering af artikel 40, stk. 1, i EU's telekodeks.

Forslaget indebærer således, at formuleringen "informationssikkerhed i offentligt tilgængelige net og tjenester" i bestemmelsen erstattes af begrebet "sikkerhed i net og tjenester", hvilket er en konsekvens af den foreslåede § 2, nr. 7. Forslaget indebærer endvidere, at bestemmelsen rettes mod udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester, hvilket er en sproglig justering som konsekvens af de foreslåede § 2, nr. 3 og 4, samt mod udbydere af NUIK-tjenester, som defineret i den foreslåede § 2, nr. 6. Der er tale om en udvidelse af kredsen af pligtsubjekter som følge af, at EU's telekodeks, modsat rammedirektivet, stiller sikkerhedskrav til udbydere af internetbaserede kommunikationstjenester, der ikke anvender numre til dirigering af opkald, beskeder, mails eller lignende.

Der kan med hjemmel i bestemmelsen fastsættes krav om, at udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester skal håndtere sikkerheden i net og tjenester gennem dokumenterede og ledelsesforankrede processer, herunder risikostyringsprocesser. Den foreslåede bemyndigelse forudsættes – som for de traditionelle teleudbydere i dag – anvendt til administrativt at fastsætte regler med nærmere krav til processerne. Der kan således administrativt stilles krav om, at processerne skal fastlægges og gennemføres efter en relevant og anerkendt international standard eller tilsvarende.

Herudover kan bemyndigelsen anvendes til at fastsætte krav om, at de omfattede udbyderes risikostyring på informationssikkerhedsområdet skal tage højde for informationssikkerhedsaspekter ved indgåelse og gennemførelse af aftaler med tredjemand om leverance af hardware, firmware eller software samt aftaler om varetagelse af driftsopgaver, der er væsentlige for udbydernes virke, eller som i øvrigt har betydning for sikkerheden i udbydernes net og tjenester. Driftsopgaver skal forstås bredt og omfatter bl.a. vedligehold og driftsovervågning. Der kan endvidere med hjemmel i bestemmelsen stilles nærmere krav til udbydernes håndtering af leverancer m.v. fra tredjemand, herunder om at udbyderne skal have dokumenterede procedurer til verificering af, at konfigurationen af det leverede hardware, firmware eller software ikke udgør en trussel mod informationssikkerheden, samt krav om, at der fastsættes dokumenterede procedurer for udbydernes kontrol med leverandørers drift af det leverede hardware, firmware eller software.

Med hjemmel i bestemmelsen kan der desuden stilles krav om, at udbydere skal sikre, at kun autoriserede (eventuelt sikkerhedsgodkendte) personer får adgang til nærmere bestemte dele af udbydernes infrastruktur, herunder f.eks. centrale dele af udbydernes net. Der kan i den forbindelse stilles krav om, at udbyderne skal fastsætte interne retningslinjer for, hvilke medarbejdere hos udbyderne og deres eventuelle leverandører, som må have adgang til udbydernes infrastruktur, ligesom der kan stilles nærmere krav til udbydernes adgangskontrol.

Det er forudsat i EU's telekodeks, at de omfattede udbydere skal træffe foranstaltninger for at beskytte sikkerheden i deres net og tjenester og for at forhindre eller minimere virkningen af sikkerhedshændelser.

I den forbindelse konstateres det i præamblens betragtning nr. 94, at sikkerhedsforanstaltningerne som minimum bør tage hensyn til alle relevante aspekter af de følgende elementer:

– vedrørende nets og faciliteters sikkerhed: fysisk og miljømæssig sikkerhed, forsyningssikkerhed, kontrol af adgang til net og netintegritet;
– vedrørende håndtering af sikkerhedshændelser: procedurer for håndtering af sikkerhedshændelser, kapacitet til detektering af sikkerhedshændelser, underretning om og meddelelse af sikkerhedshændelser;
– vedrørende styring af driftskontinuitet: strategi for tjenesters kontinuitet og beredskabsplaner, katastrofeberedskabskapacitet;
– vedrørende monitorering, audit og testning: monitorerings- og logningspolitikker, øvelsesberedskabsplaner, testning af net og tjenester, sikkerhedsvurdering og kontrol med overholdelse;
– samt overholdelse af internationale standarder.

Det fremhæves endvidere i artikel 40, stk. 1, i EU's telekodeks, at det kan være relevant at anvende kryptering som foranstaltning til at forhindre og minimere virkningen af sikkerhedshændelser.

Der er i vidt omfang tale om foranstaltninger, som allerede i dag er omfattet af bemyndigelsen i § 3, stk. 1. Det forudsættes, at den nærmere udmøntning af bemyndigelsen sker under hensyntagen til de relevante fortolkningsbidrag i EU's telekodeks.

Der vil i overensstemmelse med EU's telekodeks kunne være forskel på de krav, som fastsættes over for henholdsvis de traditionelle teleudbydere – hvilket i vidt omfang vil være en videreførelse af de nuværende krav – og de krav, som fastsættes over for udbydere af NUIK-tjenester. Det skyldes bl.a., at udbyderne af NUIK-tjenester som udgangspunkt ikke udøver egentlig kontrol over transmissionen af signaler via telenettene, og at sikkerhedskrav relateret til driften af disse net derfor ikke vil være relevante at rette mod udbydere af NUIK-tjenester.

Der henvises i øvrigt til afsnit 3.1 og 3.2 i de almindelige bemærkninger.

Til nr. 7

Det fremgår af den gældende § 3, stk. 2, at Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige net og tjenester at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod informationssikkerheden i deres risikostyringsprocesser efter stk. 1.

Der foreslås visse begrebsmæssige ændringer af § 3, *stk. 2.* Det foreslås således, at "offentligt tilgængelige net og tjenester" ændres til "offentligt tilgængelige elektroniske kommunikationsnet og -tjenester".

Forslaget er en konsekvens af den foreslåede ændring af § 2, nr. 3. Der henvises herom til bemærkningerne til § 1, nr. 4.

Derudover foreslås "informationssikkerheden" ændret til "sikkerheden i net og tjenester".

Forslaget er en konsekvens af forslaget om at anvende begrebet "sikkerhed i net og tjenester", som introduceres med EU's telekodeks, og som er defineret i den foreslåede § 2, nr. 7.

Til nr. 8

Der er ikke i dag regler, der i alle tilfælde giver Center for Cybersikkerhed mulighed for at påbyde udbydere af offentligt tilgængelige kommunikationsnet og -tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret.

Det følger af forslaget om at indsætte en ny bestemmelse som § 3, *stk. 3,* at Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse

eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret. Centeret vil være bemyndiget til at fastsætte nærmere regler herom.

Med indsættelsen af en ny bestemmelse som stk. 3 i lovens § 3, bliver det nuværende stk. 3 til stk. 4.

Bestemmelsen implementerer artikel 41, stk. 1, i EU's telekodeks.

Den foreslåede nye bestemmelse skal sikre, at der tages de nødvendige skridt til at håndtere en sikkerhedshændelse eller en betydelig trussel om en sikkerhedshændelse.

Der kan på den baggrund med hjemmel i bestemmelsen fastsættes regler om, at Center for Cybersikkerhed, når en sikkerhedshændelse er indtrådt, kan påbyde udbyderen eller udbyderen af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe sikkerhedshændelsen. Det er således en forudsætning for at anvende bestemmelsen i tilfælde af en sikkerhedshændelse, at den pågældende udbyder ikke i rette tid og af egen drift træffer de nødvendige foranstaltninger. Det vil afhænge af sikkerhedshændelsens karakter, hvilke foranstaltninger der er nødvendige for at afhjælpe denne.

Der kan endvidere med hjemmel i bestemmelsen fastsættes regler om, at Center for Cybersikkerhed, når en betydelig trussel om en sikkerhedshændelse er identificeret, kan påbyde udbyderen eller udbyderen af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at hindre sikkerhedshændelsen i at forekomme.

Det forudsættes, at de konkrete foranstaltninger, som Center for Cybersikkerhed kan påbyde i medfør af de nærmere regler, der udstedes herom, i videst muligt omfang vil være baseret på anerkendte internationale standarder eller tilsvarende.

Det vil eksempelvis kunne påbydes, at den pågældende udbyder eller udbyder af NUIK-tjenester iværksætter foranstaltninger, som er omfattet af minimumskravene i lovens § 3, stk. 1, hvis dette ikke i forvejen er sket, eller hvis det ikke er sket i det fornødne omfang. Den pågældende udbyder kan eksempelvis efter omstændighederne og i relevant omfang pålægges at sikre, at leverancer af hardware, firmware eller software, der kan udgøre en sårbarhed i den pågældende udbyders net eller tjeneste, skal undersøges for sårbarheder, samt at foretage logisk og fysisk adgangskontrol til nærmere angivne systemer eller udstyr og sikre sporbarhed heraf.

Der henvises i øvrigt til afsnit 3.3 i de almindelige bemærkninger.

Til nr. 9

Det fremgår af den gældende § 3, stk. 3, at såfremt det er af væsentlig samfundsmæssig betydning, kan Center for Cybersikkerhed påbyde udbydere af offentligt tilgængelige net og tjenester at træffe konkrete foranstaltninger med henblik på at sikre informationssikkerheden i offentligt tilgængelige net og tjenester. Centeret fastsætter nærmere regler herom.

Det følger af den foreslåede ændring af § 3, stk. 3, der fremadrettet bliver *stk. 4*, at såfremt det er af væsentlig samfundsmæssig betydning, kan Center for Cybersikkerhed påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at træffe konkrete foranstaltninger med henblik på at sikre sikkerheden i net og tjenester. Centeret fastsætter nærmere regler herom.

Det foreslås således, at formuleringen "informationssikkerheden i offentligt tilgængelige net og tjenester" i bestemmelsen erstattes af det nye begreb "sikkerheden i net og tjenester", hvilket er en konsekvens af den foreslåede § 2, nr. 7. Det foreslås endvidere, at bestemmelsen rettes mod udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester, hvilket er en sproglig justering som konsekvens af de foreslåede § 2, nr. 3 og 4.

Der henvises til bemærkningerne til lovforslagets § 1, nr. 4.

Der er i vidt omfang tale om en videreførelse af den nuværende ordning. Det EU-retlige begreb "sikkerheden i net og tjenester" indebærer dog sammenlignet med det nuværende begreb "informationssikkerhe-

den", at der også kan fastsættes påbud med henblik på sikring af autenticiteten i net og tjenester. Dette vurderes at indebære en meget beskeden udvidelse af bestemmelsens anvendelsesområde.

Til nr. 10

Det følger af den gældende § 4, 1. pkt., at Center for Cybersikkerhed fastsætter regler om oplysnings- og underretningspligter for udbydere.

Det følger af den foreslåede ændring af lovens § 4, *1. pkt.*, at udbydere af NUIK-tjenester omfattes af bestemmelsen, således at Center for Cybersikkerheds bemyndigelse til at fastsætte regler om oplysnings- og underretningspligter omfatter både udbydere og udbydere af NUIK-tjenester.

Forslaget er en konsekvens af, at udbydere af NUIK-tjenester er omfattet af de underretningsforpligtelser, der følger af artikel 40, stk. 2 og 3, i EU's telekodeks, som implementeres ved de foreslåede ændringer af lovens § 4, nr. 3-5.

Der henvises herom til bemærkningerne til lovforslagets § 1, nr. 4, og afsnit 3.2 i de almindelige bemærkninger.

Til nr. 11

Center for Cybersikkerhed er i medfør af den gældende § 4, nr. 1, bemyndiget til at fastsætte regler med krav om erhvervsmæssige udbydere af offentligt tilgængelige net og tjenesters afgivelse af oplysninger til Center for Cybersikkerhed om væsentlige dele af udbyderens net eller tjenester eller driften heraf.

Center for Cybersikkerhed er endvidere i medfør af den gældende § 4, nr. 2, bemyndiget til at fastsætte regler med krav om erhvervsmæssige udbydere af offentligt tilgængelige net og tjenesters underretning af centeret ved påtænkt indgåelse af visse typer aftaler.

Det følger af den foreslåede ændring af § 4, *nr. 1* og *2*, at "offentligt tilgængelige net og tjenesters" ændres til "offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters".

Forslaget er en konsekvens af den foreslåede ændring af § 2, nr. 3. Der henvises herom til bemærkningerne til lovforslagets § 1, nr. 4.

Til nr. 12

Center for Cybersikkerhed er i medfør af den gældende § 4, nr. 3, bemyndiget til at fastsætte regler med krav om udbydere af offentligt tilgængelige net og tjenesters underretning af centeret ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester.

Center for Cybersikkerhed er i medfør af den gældende § 4, nr. 4, bemyndiget til at fastsætte regler med krav om udbydere af offentligt tilgængelige net og tjenesters underretning af offentligheden ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester.

Der er ikke i dag – udover reguleringen på persondataområdet – regler, der pålægger udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at informere deres brugere om trusler om en sikkerhedshændelse eller mulige foranstaltninger, som brugerne kan træffe for at beskytte sig mod en trussel om en sikkerhedshændelse.

Det foreslås at ophæve § 4, nr. 3 og 4 og i stedet indsætte § 4, nr. 3-5, som nyaffattede bestemmelser.

Det følger af den foreslåede nyaffattelse af § 4, *nr. 3*, at Center for Cybersikkerhed med hjemmel i bestemmelsen kan fastsætte regler med krav om, at udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester skal underrette Center for Cybersikkerhed uden unødigt ophold om sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

Formålet med bestemmelsen er at implementere ændringerne i artikel 40, stk. 2, i EU's telekodeks, sammenholdt med den hidtidige bestemmelse i rammedirektivets artikel 13 a, stk. 3.

Sammenholdt med den gældende § 4, nr. 3, er det nyt, at udbydere af NUIK-tjenester omfattes af underretningspligten. Samtidig anvendes begrebet "sikkerhedshændelser" i stedet for det hidtidige "brud på informationssikkerheden". Forslaget er en konsekvens af den foreslåede § 2, nr. 8. Det fastslås endvidere, at underretning skal ske uden unødigt ophold.

De nærmere krav til underretningspligten vil blive udmøntet i en bekendtgørelse. Der vil i den forbindelse blive lagt vægt på eventuelle udtalelser og retningslinjer fra Den Europæiske Unions Agentur for Cybersikkerhed (herefter ENISA), som i EU's telekodeks har til opgave at fremme harmonisering på tværs af medlemsstaterne, eller fra Kommissionen.

Ved fastlæggelsen af omfanget af en sikkerhedshændelses indvirkning vil der bl.a. – direkte eller indirekte – kunne lægges vægt på antallet af brugere, der berøres af sikkerhedshændelsen, varigheden af sikkerhedshændelsen, den geografiske udbredelse med hensyn til det område, der er berørt af sikkerhedshændelsen, i hvilket omfang nettets eller tjenestens funktionsdygtighed påvirkes, og omfanget af indvirkningen på økonomiske og samfundsmæssige aktiviteter.

Center for Cybersikkerhed underretter i relevant omfang kompetente myndigheder i andre medlemsstater og ENISA om modtagne underretninger.

Underretningerne skal danne grundlag for en årlig forelæggelse af en sammenfattende rapport for Kommissionen og ENISA om de underretninger, som Center for Cybersikkerhed har modtaget efter bestemmelsen, og de foranstaltninger, der er truffet, herunder om underretning af offentligheden i medfør af den foreslåede § 4, nr. 4.

Det følger af den foreslåede nyaffattelse af § 4, *nr. 4*, at Center for Cybersikkerhed med hjemmel i bestemmelsen kan fastsætte regler med krav om, at udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester efter påbud skal underrette offentligheden ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester. Det forudsættes, at det godtgøres, at det er i offentlighedens interesse, at sikkerhedshændelsen offentliggøres.

Der kan endvidere med hjemmel i den foreslåede bestemmelse fastsættes regler om, at Center for Cybersikkerhed kan offentliggøre en sikkerhedshændelse, som centeret har fået underretning om i medfør af den foreslåede § 4, nr. 4, såfremt det er i offentlighedens interesse, at sikkerhedshændelsen offentliggøres.

Sammenholdt med den gældende § 4, nr. 4, er det nyt, at udbydere af NUIK-tjenester omfattes af underretningspligten. Samtidig anvendes begrebet "sikkerhedshændelser" i stedet for det hidtidige "brud på informationssikkerheden", hvilket er en konsekvens af den foreslåede § 2, nr. 8.

Formålet med bestemmelsen er at implementere ændringerne i artikel 40, stk. 2, i EU's telekodeks, sammenholdt med den hidtidige bestemmelse i rammedirektivets artikel 13 a, stk. 3.

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

Der foreslås indsat et nyt § 4, *nr. 5*, der indebærer, at Center for Cybersikkerhed kan fastsætte regler om, at udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester skal informere deres potentielt berørte brugere om mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe i tilfælde af en særlig og betydelig trussel om en sikkerhedshændelse i udbyderens net eller tjenester. Der kan endvidere stilles krav om, at de pågældende udbydere skal informere deres brugere om selve truslen.

Bestemmelsen implementerer EU's telekodeks artikel 40, stk. 3, der er ny sammenholdt med rammedirektivet.

Bestemmelsen indebærer, at de omfattede udbyderes potentielt berørte brugere i tilfælde af særlige og betydelige trusler skal informeres om, hvordan de kan sikre deres kommunikation, f.eks. ved at anvende bestemte typer software eller krypteringsteknologier. Kravet om informering af brugerne fritager ikke udbyderne for deres forpligtelser til for egen regning at træffe passende og øjeblikkelige foranstaltninger

for at afhjælpe sikkerhedstrusler og genoprette nettet eller tjenestens normale sikkerhedsniveau. Informationen skal stilles gratis til rådighed for brugerne.

Der henvises i øvrigt til afsnit 3.4 i de almindelige bemærkninger.

Til nr. 13

Der er i den gældende § 5, stk. 2, fastsat regler om, at erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester skal udarbejde beredskabsplaner samt planlægge og deltage i øvelsesaktiviteter.

Det følger af den foreslåede ændring af § 5, *stk. 2,* at "offentligt tilgængelige net og tjenester" ændres til "offentligt tilgængelige elektroniske kommunikationsnet og -tjenester".

Forslaget er en konsekvens af den foreslåede ændring af § 2, nr. 3. Der henvises herom til bemærkningerne til lovforslagets § 1, nr. 4.

Til nr. 14

Mobilbaseret varsling i Danmark er ikke reguleret i dag, og der er derfor heller ikke pligt for udbydere af elektroniske kommunikationstjenester i mobilnet og udbydere af mobilnet til at sikre uafbrudt transmission af offentlige advarsler.

Der foreslås indsat en ny bestemmelse som § 5 a. Der vil med hjemmel i bestemmelsen kunne fastsættes regler om, at udbydere, som i medfør af teleloven skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.

Den foreslåede bestemmelse implementerer den del af artikel 108, 2. pkt., i EU's telekodeks, hvorefter medlemsstaterne sikrer, at udbydere af talekommunikationstjenester træffer alle nødvendige foranstaltninger til at sikre uafbrudt transmission af offentlige advarsler.

Den pågældende del af bestemmelsen i artikel 108, 2. pkt., i EU's telekodeks skal ses i sammenhæng med artikel 110, der pålægger medlemsstater, der allerede har etableret offentlige varslingssystemer, at sørge for, at udbydere af mobile nummerbaserede interpersonelle kommunikationstjenester udsender offentlige advarsler til berørte slutbrugere (mobilbaseret varsling).

Forpligtelsen i artikel 110 vil blive implementeret ved en ændring af teleloven, da forpligtelsen har nær sammenhæng med eksisterende forpligtelser i teleloven i relation til bl.a. alarm- og beredskabsforhold. Det mobilbaserede varslingssystem, der etableres i medfør af artikel 110 i EU's telekodeks, skal være i brug senest den 21. juni 2022.

Det forventes, at forpligtelsen til at udsende offentlige advarsler, der indføres i teleloven, vil påhvile de såkaldte mobiloperatører, som omfatter udbydere af elektroniske kommunikationstjenester i mobilnet og udbydere af mobilnet.

Den foreslåede bestemmelse i § 5 a har til formål at sikre, at mobiloperatørerne træffer alle nødvendige foranstaltninger for at undgå, at udstyr og systemer, der anvendes i forbindelse med transmission af offentlige advarsler, afbrydes. Mobiloperatørerne vil i forlængelse af eksisterende forpligtelser til at sikre en robust teleinfrastruktur i medfør af lovens § 3, stk. 1, og § 5, stk. 1, skulle planlægge og sørge for opretholdelsen af uafbrudt transmission af offentlige advarsler, herunder i relation til udstyr og systemer, der anvendes til transmission af offentlige advarsler, bl.a. tage stilling til fremskaffelse af det nødvendige reserveudstyr, og sikring af redundans og nødstrømsforsyning.

Der henvises i øvrigt til afsnit 3.5 i de almindelige bemærkninger.

Til nr. 15

Det følger af den gældende § 6, stk. 1, at en udbyder skal indstille medarbejdere og repræsentanter for udbyderen til sikkerhedsgodkendelse hos sikkerhedsmyndigheden, når de pågældende som led i deres

konkrete opgaveløsning for udbyderen skal behandle klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til informationssikkerhed eller beredskab.

Det følger af den foreslåede ændring af § 6, *stk. 1,* at "informationssikkerhed" i lovens § 6, stk. 1, ændres til "sikkerhed i net og tjenester".

Forslaget er en konsekvens af forslaget om at anvende begrebet "sikkerhed i net og tjenester", som introduceres med EU's telekodeks, og som defineres i den foreslåede § 2, nr. 7. Der henvises herom til bemærkningerne til lovforslagets § 1, nr. 4.

Til nr. 16

Det følger af den gældende § 6, stk. 2, at erhvervsmæssige udbydere af offentligt tilgængelige net skal sikre, at medarbejdere eller repræsentanter for udbyderen, der varetager kontakten til Center for Cybersikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 5, stk. 2, i fornødent omfang sikkerhedsgodkendes efter stk. 1.

Med den foreslåede ændring af § 6, *stk. 2,* ændres "offentligt tilgængelige net" til "offentligt tilgængelige elektroniske kommunikationsnet".

Forslaget er en konsekvens af den foreslåede ændring af § 2, nr. 3. Der henvises herom til bemærkningerne til lovforslagets § 1, nr. 4.

Til nr. 17

Det følger af den gældende § 9, stk. 2, at Center for Cybersikkerhed som led i sit tilsyn kan kræve, at udbydere fremlægger alle de oplysninger og det materiale om informationssikkerhed, beredskab og sikkerhedsgodkendelse, der er nødvendige for centerets tilsynsvirksomhed, herunder til afgørelse af, om et forhold falder ind under denne lov eller regler, der er udstedt i medfør af loven.

Det følger af den foreslåede ændring af § 9, *stk. 2,* at "udbydere" ændres til "udbydere og udbydere af NUIK-tjenester".

Med bestemmelsen sikres det, at Center for Cybersikkerheds eksisterende adgang til de oplysninger, der er nødvendige til gennemførelse af centerets tilsynsvirksomhed i relation til udbydere, udvides til også at gælde udbydere af NUIK-tjenester.

Den gældende bestemmelse implementerer rammedirektivets artikel 5, stk. 1, der i EU's telekodeks er videreført som artikel 20, stk. 1. I overensstemmelse med ændringerne i EU's telekodeks vil bestemmelsen fremadrettet omfatte både de traditionelle teleudbydere og udbyderne af NUIK-tjenester.

Det foreslås endvidere som konsekvens af den foreslåede § 2, nr. 7, at "informationssikkerhed" ændres til "sikkerhed i net og tjenester".

For så vidt angår de udbydere, der er omfattet af loven i dag, er der tale om en videreførelse af den gældende ordning, idet begrebet "sikkerhed i net og tjenester" dog indebærer en vis ændring af ordningens rammer, navnlig henset til, at sikring af autenticitet særskilt kan give anledning til at kræve oplysninger og materiale herom, hvis det har betydning for centerets tilsynsvirksomhed.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 2, nr. 7, jf. lovforslagets § 1, nr. 4.

Til nr. 18

Det følger af den gældende § 9, stk. 5, at Center for Cybersikkerhed kan stille krav om, at udbydere skal foranstalte en uafhængig sikkerhedsrevision og stille resultaterne heraf til rådighed for centeret.

Det følger af den foreslåede ændring af § 9, *stk. 5,* at "udbydere" ændres til "udbydere og udbydere af NUIK-tjenester".

Bestemmelsen indebærer, at Center for Cybersikkerheds eksisterende mulighed for at kræve, at udbyde-

re skal foranstalte en uafhængig sikkerhedsrevision og stille resultaterne heraf til rådighed for centeret, udvides til også at gælde udbydere af NUIK-tjenester.

Den gældende bestemmelse implementerer rammedirektivets artikel 13 b, stk. 2, litra b, der i EU's telekodeks er videreført som artikel 41, stk. 2, litra b. I overensstemmelse med ændringerne i EU's telekodeks vil bestemmelsen fremadrettet omfatte både de traditionelle teleudbydere og udbyderne af NUIK-tjenester.

Til nr. 19

Det følger af den gældende § 9, stk. 6, at såfremt det er nødvendigt af hensyn til informationssikkerheden, har Center for Cybersikkerhed efter et skriftligt varsel på mindst syv arbejdsdage uden retskendelse mod behørig legitimation adgang til udbyderes forretningslokaler med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven. Center for Cybersikkerhed kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

Efter den gældende § 9, stk. 7, har Center for Cybersikkerhed, såfremt det er nødvendigt af hensyn til informationssikkerheden, efter et skriftligt varsel på mindst syv arbejdsdage uden retskendelse mod behørig legitimation adgang til forretningslokaler hos udbyderes samarbejdspartnere, leverandører eller underleverandører med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, i relation til outsourcet aktivitet. Center for Cybersikkerhed kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

Det foreslås, at "informationssikkerheden" i § 9, *stk. 6, 1. pkt.,* og *stk. 7, 1. pkt.,* ændres til "sikkerheden i net og tjenester". Forslaget er en konsekvens af forslaget om at anvende begrebet "sikkerhed i net og tjenester", som introduceres med EU's telekodeks, og som er defineret i den foreslåede § 2, nr. 7. Der henvises herom til bemærkningerne til lovforslagets § 1, nr. 4.

Til nr. 20

Det følger af den gældende § 10, stk. 1, nr. 1, at Center for Cybersikkerhed i ikke-anonymiseret form kan offentliggøre påbud meddelt i medfør af § 3, stk. 2 og 3, og § 5, stk. 4, og afgørelser truffet i medfør af regler, der er udstedt i medfør af § 3, stk. 1 og 3, § 4, § 5, stk. 1, 2 og 3, og § 6, stk. 6.

Med den foreslåede ændring af § 10, *stk. 1, nr. 1*, ændres "§ 3, stk. 2 og 3," til "§ 3, stk. 2, 3 og 4,", "§ 3, stk. 1 og 3," ændres til "§ 3, stk. 1, 3 og 4,", og efter "§ 5, stk. 1, 2 og 3," indsættes "§ 5 a,".

Det følger af den foreslåede ændring af § 10, *stk. 1, nr. 1,* at Center for Cybersikkerhed også i ikke-anonymiseret form kan offentliggøre påbud efter den foreslåede nye § 3, stk. 3, om påbud om konkrete foranstaltninger for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, samt afgørelser truffet i medfør af regler, der er udstedt i medfør af den nye § 3, stk. 3, samt den nye § 5 a om sikring af uafbrudt transmission af offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer.

Der foreslås i den forbindelse en konsekvensrettelse som følge af, at den gældende § 3, stk. 3, fremadrettet vil blive stk. 4.

Til nr. 21

Der er i den gældende § 10, stk. 2, fastsat regler om, at Center for Cybersikkerheds offentliggørelse af påbud og afgørelser m.v. efter stk. 1 ikke må indeholde visse oplysninger. Efter § 10, stk. 2, nr. 1, må offentliggørelse således ikke indeholde oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den udbyder, som oplysningerne angår.

Med den foreslåede ændring af § 10, *stk. 2, nr. 1,* ændres "den udbyder" til "den udbyder eller udbyder af NUIK-tjenester".

Center for Cybersikkerhed kan i medfør af lovens § 10, stk. 1, i ikke-anonymiseret form bl.a. offentliggøre henholdsvis påbud, som er meddelt i medfør af visse af lovens bestemmelser, og afgørelser, som er truffet efter bekendtgørelser, som er fastsat i medfør af visse af lovens bestemmelser. Der er tale om bestemmelser, som med lovforslaget vil omfatte både udbydere og udbydere af NUIK-tjenester, jf. lovforslagets § 1, nr. 6, 8 og 16, der henholdsvis ændrer § 3, stk. 1, og indsætter nye bestemmelser i § 3, stk. 3, og § 5 a. Det bemærkes i den forbindelse, at den gældende § 3, stk. 3, bliver stk. 4 i medfør af lovforslagets § 1, nr. 8.

Med bestemmelsen sikres det på den baggrund, at offentliggørelse efter § 10, stk. 1, ikke må indeholde oplysninger vedrørende tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign., for så vidt det er af væsentlig økonomisk betydning for den udbyder eller den udbyder af NUIK-tjenester, som oplysningerne angår.

Til nr. 22

Det følger af den gældende § 12, stk. 1, at Center for Cybersikkerhed hos udbydere kan indsamle oplysninger med henblik på at videregive disse til Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater i det omfang, det er nødvendigt for, at disse kan opfylde deres opgaver i forhold til traktatmæssige forpligtelser eller forpligtelser i henhold til den gældende EU-ret.

Efter den gældende § 12, stk. 2, orienterer Center for Cybersikkerhed de udbydere, der er indsamlet oplysninger fra, forud for videregivelse af oplysningerne til Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

Det følger af den foreslåede ændring af § 12, *stk. 1* og *2,* at "udbydere" ændres til "udbydere og udbydere af NUIK-tjenester".

Herudover foreslås "Det Europæiske Agentur for Net- og Informationssikkerhed" ændret til "Den Europæiske Unions Agentur for Cybersikkerhed". Dette skyldes, at ENISA – som det fortsat forkortes – har skiftet navn.

Med de foreslåede ændringer af bestemmelserne i stk. 1 og 2 sikres det, at der gælder samme regler for udbydere og udbydere af NUIK-tjenester i relation til udveksling af oplysninger mellem Center for Cybersikkerhed og Kommissionen, ENISA og nationale tilsynsmyndigheder i andre EU-medlemsstater.

Bestemmelserne i § 12, stk. 1 og 2, implementerer artikel 20, stk. 2, i EU's telekodeks. Derudover implementerer § 12, stk. 1, artikel 40, stk. 2, i EU's telekodeks.

Til nr. 23

Det følger af den gældende § 13, at Center for Cybersikkerhed kan fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Kommissionen vedrørende informationssikkerhed og beredskab på teleområdet, herunder regler om sanktioner i form af bøder for manglende overholdelse af retsakterne.

Med den foreslåede ændring af § 13, ændres "informationssikkerhed og beredskab på teleområdet" til "sikkerhed i net og tjenester".

Ændringen er en konsekvens af den foreslåede § 2, nr. 7.

Med forslaget videreføres Center for Cybersikkerheds hjemmel til at fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Kommissionen om sikkerhed i net og tjenester. Bemyndigelsen kan benyttes til at gennemføre retsakter, som Kommissionen i medfør af artikel 40, stk. 5, i EU's telekodeks vedtager med henblik på at udmønte foranstaltninger og underretningspligter efter artikel 40, stk. 1 og 2.

Center for Cybersikkerhed er med bestemmelsen endvidere fortsat bemyndiget til at fastsætte regler

om straf i form af bøde for overtrædelse af bestemmelser indeholdt i retsakter udstedt af Kommissionen vedrørende sikkerhed i net og tjenester. Derved sikres en effektiv gennemførelse af retsakterne.

Til nr. 24

Det er i den gældende § 14, stk. 1, nr. 1, fastsat, at undladelse af at efterkomme Center for Cybersikkerheds påbud efter lovens § 3, stk. 2 eller 3, eller § 5, stk. 4, kan straffes med bøde.

Det følger af den foreslåede ændring af § 14, *stk. 1, nr. 1,* at det også vil kunne straffes med bøde at undlade at efterkomme Center for Cybersikkerheds påbud efter den foreslåede nye § 3, stk. 3, om påbud om konkrete foranstaltninger for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme. Der foreslås endvidere en konsekvensrettelse som følge af, at den gældende § 3, stk. 3, fremadrettet bliver stk. 4.

Bestemmelsen implementerer herefter artikel 29 i EU's telekodeks om fastsættelse af sanktioner.

Til nr. 25

Center for Cybersikkerhed er i medfør af den gældende § 14, stk. 2, bemyndiget til at fastsætte straf i form af bøde for overtrædelse af bestemmelser i regler, som udfærdiges i medfør af lovens § 3, stk. 1 eller 3, § 4, § 5, stk. 1, 2 eller 3, eller § 6, stk. 6. Bestemmelsen implementerer artikel 21 a i rammedirektivet.

Det følger af den foreslåede ændring af § 14*, stk. 2,* at Center for Cybersikkerhed også bemyndiges til at fastsætte straf i form af bøde for overtrædelse af bestemmelser i regler, der udfærdiges i medfør af de foreslåede nye bestemmelser i henholdsvis § 3, stk. 3, om påbud om konkrete foranstaltninger for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, og § 5 a om sikring af uafbrudt transmission af offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer.

Der foreslås endvidere en konsekvensrettelse som følge af, at den gældende § 3, stk. 3, fremadrettet bliver stk. 4.

Bestemmelsen implementerer herefter artikel 29 i EU's telekodeks om fastsættelse af sanktioner.

Til § 2

Det foreslås, at loven træder i kraft den 21. december 2020.

Det bemærkes, at lov om net- og informationssikkerhed ikke gælder for Færøerne og Grønland og heller ikke kan sættes i kraft ved kongelig anordning. Ændringsloven vil derfor heller ikke være gældende for Færøerne og Grønland.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed foretages følgende ændringer:
	1. Lovens *titel* affattes således: **»Lov om sikkerhed i net og tjenester«.**
Lov om net- og informationssikkerhed	
Fodnoten. Loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), EU-Tidende 2002, nr. L 108, side 33, som senest ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009, samt Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet), EU-Tidende 2002, nr. L 108, side 51, som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009.	**2.** *Fodnoten* til lovens titel affattes således: »1) Loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning), EU-Tidende 2018, nr. L 321, side 36.«
§ 1. Lovens formål er at fremme net- og informationssikkerheden i samfundet.	**3.** *§ 1* affattes således: **»§ 1.** Lovens formål er at fremme sikkerheden i net og tjenester. *Stk. 2.* Henvisninger i loven og administrative forskrifter udstedt i medfør af loven til Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) med senere ændringer samt Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet) med senere ændring gælder som henvisninger til Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommu-

§ 2. I denne lov forstås ved:

1) Net: Elektroniske kommunikationsnet i form af radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af tjenester.

2) Tjeneste: Elektronisk kommunikationstjeneste, der helt eller delvis består i elektronisk overførsel af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter.

3) Offentligt tilgængelige net og tjenester: Net og tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.

4) Udbyder: Den, der med et kommercielt formål stiller produkter, net eller tjenester til rådighed for andre.

5) Erhvervsmæssig udbyder: En udbyder, der med et kommercielt formål udbyder produkter, net eller tjenester som sin hovedydelse eller som en ikke accessorisk del af virksomheden.

nikation (omarbejdning) og skal læses efter sammenligningstabellen i direktivets bilag XIII.«

4. *§ 2* affattes således:

»**§ 2.** I denne lov forstås ved:

1) Elektronisk kommunikationsnet: Transmissionssystem, uanset om det bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres.

2) Elektronisk kommunikationstjeneste: Tjeneste, der helt eller delvis består i elektronisk overførsel af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter.

3) Offentligt tilgængelige elektroniske kommunikationsnet og -tjenester: Elektroniske kommunikationsnet og -tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.

4) Udbyder: Den, der med et kommercielt formål stiller produkter, elektroniske kommunikationsnet eller -tjenester til rådighed for andre. Begrebet omfatter ikke udbydere af NUIK-tjenester, jf. nr. 6.

5) Erhvervsmæssig udbyder: En udbyder, der med et kommercielt formål udbyder produkter, elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikke accessorisk del af virksomheden. Begrebet omfatter ikke udbydere af NUIK-tjenester, jf. nr. 6.

6) Udbyder af NUIK-tjeneste: En udbyder af en nummeruafhængig interpersonel kommunikationstjeneste i form af en tjeneste, som normalt ydes

mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer, hvem modtageren eller modtagerne skal være. Omfattet er ikke tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste. Tjenesten etablerer ikke forbindelse til offentligt tildelte nummerressourcer, dvs. et eller flere numre i nationale eller internationale nummerplaner, eller muliggør ikke kommunikation med et eller flere numre i nationale eller internationale nummerplaner.

7) Sikkerhed i net og tjenester: Net og tjenesters evne til på et givet fortrolighedsniveau at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af disse net og tjenester, lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net eller tjenester.

8) Sikkerhedshændelse: En begivenhed, der har en faktisk negativ indvirkning på sikkerheden i net og tjenester.«

5. I *overskriften* til kapitel 2 ændres »Informationssikkerhed« til: »Sikkerhed«.

6. *§ 3, stk. 1,* affattes således:

»Center for Cybersikkerhed fastsætter regler om minimumskrav til sikkerhed i net og tjenester for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til sikkerhed i net og tjenester og opretholdelse af et passende sikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.«

7. I *§ 3, stk. 2,* ændres »offentligt tilgængelige net og tjenester« til: »offentligt tilgængelige elektroniske kommunikationsnet og -tjenester«, og »in-

Kapitel 2

Informationssikkerhed i net og tjenester

§ 3. Center for Cybersikkerhed fastsætter regler om minimumskrav til informationssikkerhed for udbydere af offentligt tilgængelige net og tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til informationssikkerhed i offentligt tilgængelige net og tjenester og opretholdelse af et passende informationssikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Stk. 2. Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige net og tjenester at inddrage nærmere angivne områder af de-

res virksomhed og nærmere angivne trusler mod informationssikkerheden i deres risikostyringsprocesser efter stk. 1.

Stk. 3. Såfremt det er af væsentlig samfundsmæssig betydning, kan Center for Cybersikkerhed påbyde udbydere af offentligt tilgængelige net og tjenester at træffe konkrete foranstaltninger med henblik på at sikre informationssikkerheden i offentligt tilgængelige net og tjenester. Centeret fastsætter nærmere regler herom.

§ 4. Center for Cybersikkerhed fastsætter regler om oplysnings- og underretningspligter for udbydere. Reglerne kan omfatte krav om:

1) Erhvervsmæssige udbydere af offentligt tilgængelige net og tjenesters afgivelse af oplysninger til Center for Cybersikkerhed om væsentlige dele af udbyderens net eller tjenester eller driften heraf.

2) Erhvervsmæssige udbydere af offentligt tilgængelige net og tjenesters underretning af Center for Cybersikkerhed ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf. Der kan endvidere stilles krav om, at udbyderne skal indsende et endeligt aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 10 arbejdsdage efter centerets modtagelse af dette udkast.

3) Udbydere af offentligt tilgængelige net og tjenesters underretning af Center for Cybersikkerhed ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester.

formationssikkerheden« ændres til: »sikkerheden i net og tjenester«.

8. I *§ 3* indsættes efter stk. 2 som nyt stykke:

»*Stk. 3*. Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret. Centeret fastsætter nærmere regler herom.«

Stk. 3 bliver herefter stk. 4.

9. I *§ 3, stk. 3,* der bliver stk. 4, ændres »offentligt tilgængelige net og tjenester« til: »offentligt tilgængelige elektroniske kommunikationsnet og -tjenester«, og »informationssikkerheden i offentligt tilgængelige net og tjenester« ændres til: »sikkerheden i net og tjenester«.

10. I *§ 4, 1. pkt.,* indsættes efter »for udbydere«: »og udbydere af NUIK-tjenester«.

11. I *§ 4, nr. 1 og 2,* ændres »offentligt tilgængelige net og tjenesters« til: »offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters«.

12. *§ 4, nr. 3 og 4,* ophæves, og i stedet indsættes:

»3) Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters underretning af Center for Cybersikkerhed uden unødigt ophold om sikker-

hedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

4) Udbydere af offentligt tilgængelige net og tjenesters underretning af offentligheden ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester.

4) Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters underretning af offentligheden ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

5) Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters informering af deres potentielt berørte brugere om mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe i tilfælde af en særlig og betydelig trussel om en sikkerhedshændelse i udbyderens net eller tjenester. Der kan endvidere stilles krav om, at de pågældende udbydere skal informere deres brugere om selve truslen.«

§ 5. ---

Stk. 2. For erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester kan det i regler efter stk. 1 endvidere fastsættes, at udbyderne med henblik på at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer skal

1) udarbejde beredskabsplaner baseret på en dokumenteret og ledelsesforankret risikostyringsproces og

2) planlægge og deltage i øvelsesaktiviteter.

Stk. 3-4. ---

13. I *§ 5, stk. 2,* ændres »offentligt tilgængelige net og tjenester« til: »offentligt tilgængelige elektroniske kommunikationsnet og -tjenester«.

14. Efter § 5 indsættes i *kapitel 3*:

»**§ 5 a.** Center for Cybersikkerhed fastsætter regler om, at udbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.«

§ 6. En udbyder skal indstille medarbejdere og repræsentanter for udbyderen til sikkerhedsgodkendelse hos sikkerhedsmyndigheden, når de pågældende som led i deres konkrete opgaveløsning for udbyderen skal behandle klassificerede informationer eller andre informationer, der er særligt

15. I *§ 6, stk. 1,* ændres »informationssikkerhed« til: »sikkerhed i net og tjenester«.

beskyttelsesværdige i relation til informationssikkerhed eller beredskab.

Stk. 2. Erhvervsmæssige udbydere af offentligt tilgængelige net skal sikre, at medarbejdere eller repræsentanter for udbyderen, der varetager kontakten til Center for Cybersikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 5, stk. 2, i fornødent omfang sikkerhedsgodkendes efter stk. 1.

Stk. 3-6. ---

16. I *§ 6, stk. 2,* ændres »offentligt tilgængelige net« til: »offentligt tilgængelige elektroniske kommunikationsnet«.

§ 9. ---

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

17. I *§ 9, stk. 2,* ændres »udbydere« til: »udbydere og udbydere af NUIK-tjenester«, og »informationssikkerhed« ændres til: »sikkerhed i net og tjenester«.

Stk. 3-4. ---

Stk. 5. Center for Cybersikkerhed kan stille krav om, at udbydere skal foranstalte en uafhængig sikkerhedsrevision og stille resultaterne heraf til rådighed for centeret.

18. I *§ 9, stk. 5,* ændres »udbydere« til: »udbydere og udbydere af NUIK-tjenester«.

Stk. 6. Såfremt det er nødvendigt af hensyn til informationssikkerheden, har Center for Cybersikkerhed efter et skriftligt varsel på mindst 7 arbejdsdage uden retskendelse mod behørig legitimation adgang til udbyderes forretningslokaler med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven. Center for Cybersikkerhed kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

19. I *§ 9, stk. 6, 1. pkt.,* og *stk. 7, 1. pkt.,* ændres »informationssikkerheden« til: »sikkerheden i net og tjenester«.

Stk. 7. Såfremt det er nødvendigt af hensyn til informationssikkerheden, har Center for Cybersikkerhed efter et skriftligt varsel på mindst 7 arbejdsdage uden retskendelse mod behørig legitimation adgang til forretningslokaler hos udbyderes samarbejdspartnere, leverandører eller underleverandører med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, i relation til outsourcet aktivitet. Center for Cybersikkerhed kan ikke i forbindelse med

adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

§ 10. Center for Cybersikkerhed kan i ikkeanonymiseret form offentliggøre:

1) Påbud meddelt i medfør af § 3, stk. 2 og 3, og § 5, stk. 4, og afgørelser truffet i medfør af regler, der er udstedt i medfør af § 3, stk. 1 og 3, § 4, § 5, stk. 1, 2 og 3, og § 6, stk. 6.

2-4) ---

Stk. 2. Offentliggørelse efter stk. 1 må ikke indeholde

1) oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign., for så vidt det er af væsentlig økonomisk betydning for den udbyder, som oplysningerne angår,

2-5) ---

Stk. 3. ---

§ 12. Center for Cybersikkerhed kan hos udbydere indsamle oplysninger med henblik på at videregive disse til Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater, i det omfang det er nødvendigt, for at disse kan opfylde deres opgaver i forhold til traktatmæssige forpligtelser eller forpligtelser i henhold til den gældende EU-ret.

Stk. 2. Center for Cybersikkerhed orienterer de udbydere, der er indsamlet oplysninger fra, forud for videregivelse af oplysningerne til Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

Stk. 3. ---

§ 13. Center for Cybersikkerhed kan fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Kommissionen vedrørende informationssikkerhed og beredskab på teleområdet, herunder regler om sanktioner i form af bøder for manglende overholdelse af retsakterne.

20. I *§ 10, stk. 1, nr. 1,* ændres »§ 3, stk. 2 og 3,« til »§ 3, stk. 2, 3 og 4,«, »§ 3, stk. 1 og 3,« ændres til: »§ 3, stk. 1, 3 og 4,«, og efter »§ 5, stk. 1, 2 og 3,« indsættes: »§ 5 a,«.

21. I *§ 10, stk. 2, nr. 1,* ændres »den udbyder« til: »den udbyder eller udbyder af NUIK-tjenester«.

22. I *§ 12, stk. 1* og *2,* ændres »udbydere« til: »udbydere og udbydere af NUIK-tjenester«, og »Det Europæiske Agentur for Net- og Informationssikkerhed« ændres til »Den Europæiske Unions Agentur for Cybersikkerhed«.

23. I *§ 13* ændres »informationssikkerhed og beredskab på teleområdet« til: »sikkerhed i net og tjenester«.

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

1) undlader at efterkomme Center for Cybersikkerheds påbud efter § 3, stk. 2 eller 3, eller § 5, stk. 4,

2) ---

Stk. 2. I regler, som udfærdiges i medfør af § 3, stk. 1 eller 3, § 4, § 5, stk. 1, 2 eller 3, eller § 6, stk. 6, kan der fastsættes straf i form af bøde for overtrædelse af bestemmelserne i reglerne.

Stk. 3. ---

24. I *§ 14, stk. 1, nr. 1,* ændres »§ 3, stk. 2 eller 3« til: »§ 3, stk. 2, 3 eller 4«.

25. I *§ 14, stk. 2,* ændres »§ 3, stk. 1 eller 3« til: »§ 3, stk. 1, 3 eller 4«, og efter »§ 5, stk. 1, 2 eller 3,« indsættes: »§ 5 a,«.