Lovtidende A

2021

Udgivet den 3. februar 2021

1. februar 2021. Nr. 153.

Bekendtgørelse af lov om sikkerhed i net og tjenester[1)]

Herved bekendtgøres lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed med de ændringer, der følger af lov nr. 1831 af 8. december 2020.

Kapitel 1

Formål og definitioner

§ 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.

§ 2. I denne lov forstås ved:

1) Elektronisk kommunikationsnet: Transmissionssystem, uanset om det bygger på en permanent infrastruktur eller en 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, og 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, og 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.

[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.

AG000968

Forsvarsmin., j.nr. 2020/009029

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

Kapitel 2

Sikkerhed i net og tjenester

§ 3. 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.

Stk. 2. Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net og tjenester i deres risikostyringsprocesser efter stk. 1.

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. 4. 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.

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

1) Erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet 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 elektroniske kommunikationsnet 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 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.

Kapitel 3

Elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer

§ 5. Center for Cybersikkerhed fastsætter regler om, at udbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Stk. 2. For erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet 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. Center for Cybersikkerhed koordinerer og prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Center for Cybersikkerhed kan fastsætte regler om, at erhvervsmæssige udbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Stk. 4. I beredskabssituationer og i andre ekstraordinære situationer kan Center for Cybersikkerhed påbyde erhvervsmæssige udbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller trussel, der i betydeligt omfang påvirker eller kan påvirke udbuddet af net eller tjenester negativt.

§ 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.

Kapitel 4

Sikkerhedsgodkendelse

§ 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 klassifice-

rede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til sikkerhed i net og tjenester eller beredskab.

Stk. 2. Erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet 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. Udbydere, hvis medarbejdere eller repræsentanter sikkerhedsgodkendes efter stk. 1, skal sikre overholdelse af sikkerhedsmyndighedens anvisninger om behandling af klassificerede informationer.

Stk. 4. Udbydere, hvis medarbejdere eller repræsentanter sikkerhedsgodkendes efter stk. 1, skal uden ugrundet ophold underrette sikkerhedsmyndigheden, når sikkerhedsgodkendte personer ikke længere varetager de opgaver for udbyderen, som lå til grund for sikkerhedsgodkendelsen.

Stk. 5. Sikkerhedsmyndigheden kan tilbagekalde en sikkerhedsgodkendelse, når betingelserne for sikkerhedsgodkendelse ikke længere er til stede.

Stk. 6. Center for Cybersikkerhed kan fastsætte regler om sikkerhedsgodkendelse af udbyderes medarbejdere eller repræsentanter for udbydere, der har adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelseshemmeligheden.

Kapitel 5

Aktindsigt i underretninger m.v.

§ 7. Det kan i regler udstedt i medfør af § 4 fastsættes, at underretninger og afgivelse af oplysninger efter § 4, nr. 1-3, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

§ 8. Myndigheder og virksomheder kan 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.

Stk. 2. Underretninger efter stk. 1 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Kapitel 6

Tilsyn m.v.

§ 9. Center for Cybersikkerhed fører tilsyn med overholdelsen af denne lov og regler, der er udstedt i medfør af loven.

Stk. 2. Center for Cybersikkerhed kan som led i sit tilsyn kræve, at udbydere og udbydere af NUIK-tjenester fremlægger alle de oplysninger og det materiale om sikkerhed i net og tjenester, 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.

Stk. 3. Center for Cybersikkerhed kan stille krav om, hvordan og i hvilken form oplysninger og materiale efter stk. 2 skal afgives.

Stk. 4. Center for Cybersikkerhed kan afkræve udbydere skriftlige udtalelser og redegørelser om faktiske forhold af betydning for centerets tilsynsvirksomhed.

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

Stk. 6. Såfremt det er nødvendigt af hensyn til sikkerheden i net og tjenester, 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.

Stk. 7. Såfremt det er nødvendigt af hensyn til sikkerheden i net og tjenester, 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, 3 og 4, og § 5, stk. 4, og afgørelser truffet i medfør af regler, der er udstedt i medfør af § 3, stk. 1, 3 og 4, § 4, § 5, stk. 1, 2 og 3, § 5 a og § 6, stk. 6.
2) Resultater af tilsyn efter § 9.
3) Resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov.
4) Resumeer af domme i retssager, hvor Center for Cybersikkerhed er part.

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 eller udbyder af NUIK-tjenester, som oplysningerne angår,
2) oplysninger, der er af væsentlig betydning for statens sikkerhed eller rigets forsvar,
3) klassificerede informationer,
4) fortrolige oplysninger, der hidrører fra nationale tilsynsmyndigheder i andre EU-medlemsstater, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse til offentliggørelse, eller
5) oplysninger om enkeltpersoners forhold.