Lovtidende A

2015

Udgivet den 16. december 2015

15. december 2015. Nr. 1567.

Lov om net- og informationssikkerhed[1)]

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

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

Kapitel 1

Formål og definitioner

§ 1. Lovens formål er at fremme net- og informationssikkerheden i samfundet.

§ 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.

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 deres 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.

[1)] 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.

AG000685

Forsvarsmin., j.nr. 2015/005940

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.

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 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. 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.

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 klassificerede informationer eller andre informationer, der er særligt 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. 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 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.

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 skal foranstalte en uafhængig sikkerhedsrevision og stille resultaterne heraf til rådighed for centeret.

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.