LOV nr 1156 af 08/06/2021 (Gældende)

Lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Ministerium: Forsvarsministeriet

Journalnummer: Forsvarsmin., j.nr. 2020/008733

Lov om leverandørsikkerhed i den kritiske teleinfrastruktur

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

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

Kapitel 1

Definitioner

§ 1. I denne lov forstås ved:

1) Kritiske netkomponenter, systemer og værktøjer: Operations support-systemer, network management-systemer og business support-systemer, der kan benyttes til at aflæse, ændre indhold af eller dirigere data, som relaterer sig til slutbrugere, samt hardware, firmware og software, der anvendes i eller i forbindelse med core-net i mobilnet, fastnet og internet eller i centrale routere og servere i backbone-nettene eller i kontrolenheder, som anvendes til styring i mobilnettenes radionet.
2) Slutbruger: En bruger af net og tjenester, som ikke på kommercielt grundlag stiller de pågældende net og tjenester til rådighed for andre.
3) Væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester:
   a) Udbyder af net, hvor disse net anvendes af mere end 50.000 slutbrugere. Ved opgørelsen medregnes de slutbrugere, der har aftaleforhold med udbyderens kunder. Radio- og tv-stationer, der er udbydere af net, er kun omfattet, hvis de har landsdækkende public service-forpligtelser.
   b) Udbyder, der gennem aftaler med statslige myndigheder og institutioner betjener mere end 500 slutbrugere. Ved opgørelsen medregnes de statslige myndigheders og institutioners egne slutbrugere.

Kapitel 2

Nedlæggelse af forbud af hensyn til leverandørsikkerhed i den kritiske teleinfrastruktur

§ 2. Center for Cybersikkerhed kan i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, hvis aftalen vurderes at udgøre en trussel mod statens sikkerhed.

Stk. 2. Ved vurderingen efter stk. 1 kan Center for Cybersikkerhed lægge vægt på forhold vedrørende den leverandør, som udbyderen ønsker at anvende. I vurderingen vil bl.a. kunne indgå, om leverandøren, leverandørens væsentligste underleverandører og aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren,

1) er hjemmehørende i eller varetager produktionen eller driften fra et land, som Danmark ikke har indgået en sikkerhedsaftale med, eller som Danmark ikke har et tilsvarende sikkerhedsmæssigt samarbejde med,
2) er hjemmehørende i eller varetager produktionen eller driften fra et land, hvor det efter det pågældende lands lovgivning er muligt at pålægge leverandører eller deres underleverandører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage,
3) direkte eller indirekte kontrolleres af et andet lands statslige organer, herunder militære myndigheder, og
4) er eller har været involveret i aktiviteter i Danmark eller andre lande, som har medført en negativ påvirkning af statens sikkerhed, informationssikkerheden eller den offentlige orden.

Stk. 3. Center for Cybersikkerhed kan kun nedlægge forbud efter stk. 1, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

§ 3. Center for Cybersikkerhed kan i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at opretholde en indgået aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, hvis opretholdelse af aftalen vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed lægge vægt på de forhold, som fremgår af § 2, stk. 2.

Stk. 2. Center for Cybersikkerhed kan endvidere i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at anvende kritiske netkomponenter, systemer og værktøjer, der er leveret, hvis anvendelsen vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed lægge vægt på de forhold, som fremgår af § 2, stk. 2.

Stk. 3. Center for Cybersikkerhed kan fastsætte en frist for, hvornår en aftale skal være afviklet efter stk. 1, og hvornår anvendelse af kritiske netkomponenter, systemer og værktøjer skal være ophørt efter stk. 2.

Stk. 4. Center for Cybersikkerhed kan kun nedlægge forbud efter stk. 1 og 2, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

Kapitel 3

Ekspropriation

§ 4. Center for Cybersikkerhed kan i det omfang, det er nødvendigt for gennemførelse af forbud efter kapitel 2, iværksætte ekspropriation af privat ejendom.

Stk. 2. Udgør gennemførelse af forbud efter kapitel 2 et ekspropriativt indgreb, ydes der fuldstændig erstatning til den eller de berørte parter.

Kapitel 4

Forholdet til anden lovgivning samt høring af andre myndigheder

§ 5. Lov om offentlighed i forvaltningen bortset fra lovens § 13 og forvaltningslovens kapitel 4-6 finder ikke anvendelse på sager, der er omfattet af denne lov, jf. dog stk. 2.

Stk. 2. Center for Cybersikkerhed skal i forbindelse med afgørelser efter kapitel 2, 3 og 8 i størst muligt omfang foretage partshøring, jf. forvaltningslovens kapitel 5, og begrunde afgørelserne, jf. forvaltningslovens kapitel 6.

Stk. 3. Center for Cybersikkerhed skal forud for afgørelser efter kapitel 2 gennemføre en høring af Erhvervsstyrelsen, Energistyrelsen og andre relevante fagmyndigheder.

Kapitel 5

Fravigelse af klageadgang

§ 6. Center for Cybersikkerheds afgørelser efter kapitel 2 og 3 kan ikke påklages til anden administrativ myndighed.

Kapitel 6

Domstolsbehandling

§ 7. Afgørelser efter kapitel 2, 3 og 8 kan alene indbringes for Københavns Byret.

Stk. 2. Afgørelsen skal indbringes inden 6 måneder efter afgørelsens meddelelse. Københavns Byret kan dog undtagelsesvis tillade en indbringelse efter 6 måneder.

Stk. 3. I afgørelsen af sagen ved byretten deltager tre dommere.

Stk. 4. Forsvarsministeren eller den, ministeren bemyndiger hertil, kan lade personer, der er ansat i Forsvarsministeriet eller myndigheder under Forsvarsministeriet, møde for sig i retten som rettergangsfuldmægtige.

§ 8. Som part i sagen for det offentlige anses forsvarsministeren eller den, ministeren bemyndiger hertil.

Stk. 2. Retten beskikker en særlig advokat til at varetage interesser for den, der har indbragt sagen for retten, eller som er indtrådt som part i sagen, og på vegne af denne udøve partsbeføjelser med hensyn til oplysninger af betydning for statens sikkerhed. Om salær og godtgørelse for udlæg til den særlige advokat gælder samme regler som i tilfælde, hvor der er meddelt fri proces, jf. retsplejelovens kapitel 31.

Stk. 3. Den særlige advokat efter stk. 2 skal underrettes om alle retsmøder i sagen og er berettiget til at deltage i disse. Den særlige advokat skal gøres bekendt med og have udleveret kopi af det materiale, som indgår i sagen for retten. Forsvarsministeren eller den, ministeren bemyndiger hertil, kan dog bestemme, at der af sikkerhedsmæssige grunde ikke udleveres kopi til den særlige advokat. Spørgsmålet kan af den særlige advokat indbringes for retten.

§ 9. Oplysninger vedrørende statens sikkerhed videregives ikke til parten, men alene til den særlige advokat efter § 8, stk. 2. Når sådanne oplysninger er videregivet til den særlige advokat, må vedkommende ikke drøfte sagen med parten eller dennes advokat og må ikke udtale sig i retsmøder, hvor parten eller dennes advokat er til stede. Parten og dennes advokat kan til enhver tid give skriftlige meddelelser til den særlige advokat om sagen.

Stk. 2. Retten kan af egen drift eller efter begæring fra den særlige advokat efter § 8, stk. 2, beslutte, at oplysninger, der er indgået i vurderingen ved afgørelser omfattet af kapitel 2, 3 og 8, videregives til parten og dennes advokat, hvis sikkerhedsmæssige forhold ikke kan begrunde, at oplysningerne ikke videregives. Afgørelsen træffes ved kendelse, og efter at den særlige advokat og forsvarsministeren eller den, ministeren bemyndiger hertil, har haft lejlighed til at udtale sig. Kendelsen kan kæres af de personer, der er nævnt i 2. pkt. Kære af en afgørelse om, at oplysninger videregives, har opsættende virkning.

Stk. 3. Har retten truffet afgørelse efter stk. 2, 1. pkt., kan forsvarsministeren eller den, ministeren bemyndiger hertil, bestemme, at de pågældende oplysninger ikke indgår i sagen for retten.

Stk. 4. Ingen må deltage som dommer i sagen, hvis den pågældende har truffet afgørelse efter stk. 2, 1. pkt., eller i øvrigt har haft adgang til oplysninger omfattet af en sådan afgørelse og forsvarsministeren eller den, ministeren bemyndiger hertil, har truffet beslutning efter stk. 3 om, at de pågældende oplysninger ikke indgår i sagen for retten.

§ 10. Den del af et retsmøde, der angår eller hvori der fremlægges eller behandles oplysninger af betydning for statens sikkerhed, som ikke er omfattet af en beslutning efter § 9, stk. 2, holdes for lukkede døre. I denne del af et retsmøde deltager den særlige advokat efter § 8, stk. 2, men ikke parten og dennes advokat.

Stk. 2. Retten bestemmer, hvordan retsmøder, der efter stk. 1 helt eller delvis holdes for lukkede døre, gennemføres.

§ 11. Retten træffer afgørelse, efter at parterne og den særlige advokat har haft lejlighed til at udtale sig.

§ 12. Justitsministeren antager et antal advokater, der kan beskikkes efter § 8, stk. 2, 1. pkt. Justitsministeren kan fastsætte nærmere regler om de pågældende advokater, herunder om vagtordninger, om vederlag for at stå til rådighed og om sikkerhedsmæssige spørgsmål.

§ 13. Reglerne i dette kapitel om sagens behandling i byretten gælder tilsvarende for sagens behandling i landsretten og Højesteret.

Kapitel 7

Offentliggørelse af afgørelser m.v.

§ 14. Center for Cybersikkerhed kan i ikkeanonymiseret form offentliggøre følgende:

1) Afgørelser truffet i medfør af kapitel 2, 3 og 8.
2) Resuméer af domme i retssager, der vedrører prøvelse af afgørelser efter kapitel 2, 3 og 8.

Stk. 2. Forsvarsministeren kan fastsætte nærmere regler om sagsbehandlingen i forbindelse med offentliggørelse efter stk. 1.

Kapitel 8

Sanktioner

§ 15. Hvis en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester ikke efterlever et forbud efter § 2, stk. 1, eller § 3, stk. 1 eller 2, kan Center for Cybersikkerhed træffe afgørelse om at afsætte medlemmer af udbyderens ledelse.

Kapitel 9

Ugyldighed

§ 16. Aftaler, der er i strid med et forbud efter § 2, stk. 1, eller § 3, stk. 1, er uden gyldighed mellem parterne.

Kapitel 10

Ikrafttrædelse m.v.

§ 17. Loven træder i kraft den 1. juli 2021.

Stk. 2. §§ 1, 3-17 og 19 har virkning for aftaler, der er indgået den 7. december 2020 eller senere, jf. dog stk. 3.

Stk. 3. §§ 1, 3-17 og 19 har fra den 1. januar 2026 endvidere virkning for aftaler, der er indgået før den 7. december 2020.

Stk. 4. Forsvarsministeren udarbejder en rapport om erfaringerne med loven, som oversendes til Folketinget 3 år efter lovens ikrafttræden.

Kapitel 11

Ændring af anden lovgivning

§ 18. I lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, foretages følgende ændring:

1. I *§ 4, nr. 2, 2. pkt.,* ændres »10« til: »25«.

Kapitel 12

Lovens territoriale gyldighed

§ 19. Loven gælder ikke for Færøerne og Grønland.

Givet på Christiansborg Slot, den 8. juni 2021

Under Vor Kongelige Hånd og Segl

MARGRETHE R.

/ Trine Bramsen