

Indhold

1. Uddrag af loven om ændring af loven om elektronisk kommunikation, byggeloven og loven om statsafgifter — side 2.

Forklaring: Dette afsnit indeholder de retlige bestemmelser vedrørende gennemførelsen af 5G-værktøjskassen. Bestemmelserne til gennemførelse af Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 er udgået.

Den fulde ordlyd af loven om ændring af loven om elektronisk kommunikation, byggeloven og loven om statsafgifter findes her: <https://www.riigiteataja.ee/akt/115122021001>.

Den nuværende fulde ordlyd af loven om elektronisk kommunikation findes her: <https://www.riigiteataja.ee/akt/122102021015?leiaKehtiv>.

2. Forskrift nr. 119 af 16. december 2021 fra republikkens regering om ændring af forskrift nr. 140 af 22. juni 2006 fra republikkens regering om kravene til levering af kommunikationstjenester og om de tekniske krav til kommunikationsnetværk og forskrift nr. 129 af 11. december 2015 fra republikkens regering om statuten for sikkerhedskommissionen under republikkens regering – s. 5.

1. Uddrag af loven om ændring af loven om elektronisk kommunikation, byggeloven og loven om statsafgifter.

§ 1. Ændring af loven om elektronisk kommunikation

I loven om elektronisk kommunikation foretages følgende ændringer:

111) Afsnit 87, stk. 2¹ og 2², ophæves.

118) Loven suppleres med § 87³ til § 87⁵ med følgende ordlyd:

"§ 87³. Krav til kommunikationsnetværk og -tjenester med henblik på sikring af den nationale sikkerhed

(1) Hardware og software, der bruges til levering af kommunikationstjenester i et kommunikationsnetværk, må ikke udgøre en risiko for den nationale sikkerhed.

(2) Hardware og software, der bruges til levering af kommunikationstjenester i et kommunikationsnetværk, kan udgøre en risiko for den nationale sikkerhed på grund af:

- 1) en høj risiko, der opstår fra producenten eller leverandøren af vedligeholdelses- eller støttetjenester (i det følgende benævnt *højrisikohardware eller -software*)
- 2) en risiko som følge af hardwarens eller softwarens tekniske karakteristika eller konfiguration.

3)) Ved vurderingen af højrisikohardware eller -software tages der bl.a. hensyn til oplysninger om:

1) at producenten eller leverandøren af vedligeholdelses- eller støttetjenester har sit vedtægtsmæssige hjemsted eller hovedkontor i et land (i det følgende benævnt *bopælsland*), som ikke er medlem af Den Europæiske Union, Den Nordatlantiske Traktats Organisation (i det følgende benævnt *NATO*) eller Organisationen for Økonomisk Samarbejde og Udvikling (i det følgende benævnt *OECD*)

2) at de demokratiske retsstatsprincipper ikke overholdes, eller at menneskerettighederne ikke overholdes i det land, hvor producenten eller leverandøren af vedligeholdelses- eller støttetjenester har bopæl

3) at intellektuelle ejendomsrettigheder, personoplysninger eller forretningshemmeligheder for personer fra andre lande ikke er beskyttet i det land, hvor producenten eller leverandøren af vedligeholdelses- eller støttetjenester har bopæl

4) at producenten eller leverandøren af vedligeholdelses- eller støttetjenesters bopælsland udviser aggressiv adfærd i cyberspace

5) at den Europæiske Unions medlemsstater, NATO eller OECD har tilskrevet cyberangreb til producenten eller leverandøren af vedligeholdelses- eller støttetjenesters bopælsland

6) at producenten eller leverandøren af vedligeholdelses- eller støttetjenester er underlagt regeringen eller den statslige myndighed i bopælslandet eller et andet fremmed land, som ikke har nogen uafhængig retslig kontrol

7) at producenten eller leverandøren af vedligeholdelses- eller støttetjenesters bopælsland eller et andet fremmed land kan forpligte producenten til at handle på en måde, der udgør en risiko for Estlands nationale sikkerhed

8) at producenten eller leverandøren af vedligeholdelses- eller støttetjenesters økonomiske aktiviteter ikke er baseret på markedsbaseret konkurrence, eller der ikke er skabt passende betingelser herfor i bopælslandet

9) at producenten eller leverandøren af vedligeholdelses- eller støttetjenesters ejerstruktur,

organisationsstruktur eller ledelsesstruktur ikke er gennemsigtig

10) at finansieringen af producenten eller leverandøren af vedligeholdelses- eller støttetjenester ikke er gennemsigtig

11) at producenten eller leverandøren af vedligeholdelses- eller støttetjenesters produkter eller tjenester omfatter sårbarheder, og der er ikke truffet passende sikkerhedsforanstaltninger til at forhindre disse

12) at producenten eller leverandøren af vedligeholdelses- eller støttetjenester ikke er i stand til at sikre fortsatte leverancer af produkter eller tjenester, undtagen på grund af force majeure.

(4) Med henblik på sikring af den nationale sikkerhed er en kommunikationsvirksomhed forpligtet til at oplyse forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed om den hardware og software, der anvendes i kommunikationsnetværket.

(5) Omfanget af den meddelelsespligt, der er anført i stk. 4 i dette afsnit, samt de specifikke krav, fristen for overholdelse af forpligtelsen og proceduren for meddelelse er fastsat ved en forskrift udstedt af republikkens regering.

(6) Med henblik på sikring af den nationale sikkerhed er en kommunikationsvirksomhed forpligtet til at ansøge om en tilladelse til brug af hardware eller software i et kommunikationsnetværk (i det følgende benævnt *tilladelse til brug af hardware eller software*) fra forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed.

(7) Omfanget af forpligtelsen til at ansøge om en tilladelse til brug af hardware eller software, de specifikke krav, procedurefristen og selve proceduren samt specifikationerne vedrørende betingelserne for tilladelsen til brug er fastsat ved en forskrift udstedt af republikkens regering.

(8) Ved udstedelsen af forskrifterne i stk. 5 og 7 i denne lov tager republikkens regering hensyn til betydningen af kommunikationsnetværket, dets hardware eller software og kommunikationstjenester, der udbydes i netværket, samt de potentielle risici, der kan opstå i forbindelse hermed for den nationale sikkerhed.

§ 87⁴. Procedure vedrørende tilladelse af brug af hardware eller software

(1) Efter modtagelse af en ansøgning om tilladelse til brug af hardware eller software anmoder forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed om udtalelser fra sikkerhedsmyndighederne og informationssystemmyndigheden om, hvorvidt den hardware eller software, der er specificeret i kommunikationsvirksomhedens ansøgning om tilladelse til brug af hardware eller software, udgør en risiko for den nationale sikkerhed. Hvis hardwaren eller softwaren kan udgøre en risiko for den nationale sikkerhed i henhold til den modtagne udtalelse, anmoder forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed om godkendelse fra den myndighed, der er angivet i statuten for sikkerhedskommissionen under Republikken Estland (i det følgende benævnt: *administrative myndighed*), inden der træffes afgørelse om kommunikationsvirksomhedens ansøgning om tilladelse til brug af hardwaren eller softwaren.

(2) I den godkendelsesproces, der er angivet i stk. 1 i dette afsnit, vurderer den administrative myndighed, om brugen af den hardware eller software, der er angivet i ansøgningen om tilladelse til brug af hardwaren eller softwaren, udgør en risiko for den nationale sikkerhed. Under godkendelsesprocessen kan den administrative myndighed foreslå at forbyde brugen af den hardware eller software, der er angivet i ansøgningen om tilladelse til brug af hardware eller software, eller at fastsætte betingelser for deres brug. Betingelserne for brug af hardware

eller software kan bl.a. omfatte en tidsbegrænsning for brug, brug i visse dele eller funktioner eller med visse konfigurationer af kommunikationsnetværket.

(3) Under hensyntagen til bestemmelserne i stk. 1 og 2 i dette afsnit træffer forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed afgørelse om godkendelse, betinget godkendelse eller afslag på godkendelse af ansøgningen om tilladelse til brug af hardware eller software.

(4) Hvis hardware eller software ikke udgør en risiko for den nationale sikkerhed, gives der tilladelse til brug i otte år. Hvis hardware eller software udgør en risiko for den nationale sikkerhed, gives der ingen tilladelse til brug, eller der gives en betinget tilladelse til brug.

§ 87⁵. Revision

Stk. 1. En kommunikationsvirksomhed, for hvem der er pålagt forpligtelser på grundlag af § 87³ i denne lov, påbyder lovmæssig revision af sine aktiviteter mindst hvert tredje år efter pålæggelse af forpligtelsen, til vurdering i revisionsrapporten, om kommunikationsvirksomheden har opfyldt de forpligtelser, der er pålagt på grundlag af samme afsnit.

Stk. 2. Den person, der udfører revisionen, skal være en uafhængig revisor, der er i besiddelse af en attest fra ISACA eller en lignende attest.

Stk. 3. Den person, der udfører revisionen, forelægger revisionen for forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed.

Stk. 4. Omkostningerne ved gennemførelsen af revisionen dækkes af kommunikationsvirksomheden.

Stk. 5. Indholdet af den revisionsforpligtelse, der er anført i stk. 1 i dette afsnit, og tidspunktet og proceduren for indgivelse af revisionen er fastsat ved en forskrift udstedt af republikkens regering."

152) Loven suppleres med § 170³ med følgende ordlyd:

"§ 170³. Tilsidesættelse af forpligtelser pålagt af hensyn til den nationale sikkerhed

(1) Tilsidesættelse af forpligtelser pålagt på grundlag af § 87³ eller 87⁵ i denne lov straffes med en bøde på op til 300 bødeenheder.

(2) Den samme handling kan, hvis den begås af en juridisk person, straffes med en bøde på op til 50 000 EUR."

156) Loven suppleres med § 196³ til § 196⁵ med følgende ordlyd:

§ 196⁵. Gennemførelse af § 87³ og § 87⁴ i denne lov

(1) Forpligtelsen til at ansøge om tilladelse til brug af hardware eller software som nævnt i § 87, stk. 6³, i denne lov finder anvendelse på hardware eller software, der er taget i brug før den 1. februar 2022, hvis en funktion af ikke-selvstændig-5G (i det følgende benævnt: 5G-NSA) eller en nyere generation af mobilkommunikationsnetværksstandard er blevet eller ville blive udrullet i hardwaren eller softwaren.

(2) Højriskohardware eller -software, hvor en funktion fra 5G-NSA eller en nyere generation af mobilkommunikationsnetværksstandard bruges eller vil blive udrullet, og som ikke har en kritisk funktion, kan bruges på grundlag af en tilladelse til brug indtil den 31. december 2025.

Der udstedes ikke tilladelse til brug til højrisikohardware eller -software angivet i første punktum efter den 31. december 2025. Fristen for indgivelse af ansøgninger om tilladelse til brug af højrisikohardware eller -software angivet i første punktum fastsættes i den i § 87³, stk. 7, nævnte forskrift i denne lov.

(3) Hardware eller software, der ikke har en funktion fra 5G-NSA eller en nyere generation af mobilkommunikationsnetværksstandarden eller en kritisk funktion, kan bruges indtil den 31. december 2029 uden at ansøge om tilladelse til brug som specificeret i § 87, stk. 6³, i denne lov.

(4) Hvis den hardware eller software, der er anført i stk. 3 i dette afsnit, er beregnet til at blive brugt efter den 31. december 2029, skal en ansøgning om tilladelse til brug indgives senest den 1. juli 2029. Der udstedes ikke tilladelse til brug til højrisikohardware eller -software angivet i første punktum efter den 31. december 2029.

(5) De kritiske funktioner for hardware og software er: 1) hovednetværksfunktionen i overensstemmelse med Det Europæiske Standardiseringsinstitut for Telekommunikations standarder, uanset placeringen af funktionen i kommunikationsnetværket 2) den funktion, der har til formål at gøre det muligt for sikkerhedsmyndigheder og overvågningsmyndigheder at udføre overvågningsaktiviteter eller begrænse retten til fortrolighed af meddelelser i de tilfælde, der er fastsat ved lov."

2. Forskrift nr. 119 af 16. december 2021 fra republikkens regering om ændring af forskrift nr. 140 af 22. juni 2006 fra republikkens regering om kravene til levering af kommunikationstjenester og om de tekniske krav til kommunikationsnetværk og forskrift nr. 129 af 11. december 2015 fra republikkens regering om statuten for sikkerhedskommissionen under republikkens regering

Udsteder: REGERINGEN I REPUBLIKKEN

Type: forskrift

Teksttype: foreløbig tekst

Ikrafttræden: 1. februar 2022

Udgivelsens benævnelse: RT I, 21.12.2021, 1

Ændring af forskrift nr. 140 af 22. juni 2006 fra republikkens regering om kravene til levering af kommunikationstjenester og om de tekniske krav til kommunikationsnetværk og forskrift nr. 129 af 11. december 2015 fra republikkens regering om statuten for sikkerhedskommissionen under republikkens regering

Vedtaget den 16. december 2021, nr. 119

Forskriften fastlægges på grundlag af § 87, stk. 2, § 87³, stk. 5 og 7, og § 87⁵, stk. 5, i lov om elektronisk kommunikation og § 4, stk. 2, i lov om nationalt forsvar.

§ 1. Ændring af forskrift nr. 140 af 22. juni 2006 fra republikkens regering om kravene til levering af kommunikationstjenester og om de tekniske krav til kommunikationsnetværk

Der foretages følgende ændringer af forskrift nr. 140 af 22. juni 2006 fra republikkens regering om kravene til levering af kommunikationstjenester og om de tekniske krav til kommunikationsnetværk:

1) I § 2, stk. 1, § 3, stk. 4, nr. 1), og § 6, stk. 1, i præamblen til forskriften ændres "lov om elektronisk kommunikation" til "lov om elektronisk kommunikation".

2) I forskriftens præambel suppleres efter ordlyden "stk. 2" af ordlyden ", § 87³, stk. 5 og 7, og § 87⁵, stk. 5".

3) Afsnit 1 har følgende ordlyd:

"Nærværende forskrift fastlægger:

1) kravene til levering af offentlige elektroniske kommunikationstjenester (i det følgende benævnt: *kommunikationstjenester*), som følger af de formål, der er anført i § 87, stk. 2, nr. 1), 3) og 4), i lov om elektronisk kommunikation

2) tekniske og nationale sikkerhedskrav til et offentligt elektronisk kommunikationsnetværk (i det følgende benævnt: *kommunikationsnetværk*)

3) en forpligtelse til at oplyse om hardware og software, der bruges i kommunikationsnetværket, indholdet og proceduren for ansøgning om tilladelse til brug samt indholdet af og proceduren for en revisionsforpligtelse."

4) Forskriften suppleres med kapitel 2¹, der har følgende ordlyd:

"Kapitel 21.

KRAV TIL KOMMUNIKATIONSTJENESTER OG KOMMUNIKATIONSNETVÆRK MED HENBLIK PÅ SIKRING AF DEN NATIONALE SIKKERHED

Del 1

Almindelige bestemmelser

§ 3¹ Kravenes anvendelsesområde

(1) De fastlagte krav i dette kapitel finder anvendelse på et kommunikationsselskab, der udbyder en kritisk tjeneste i henhold til § 87, stk. 4, i lov om elektronisk kommunikation, eller som anvender 5G-NSA eller en højere generation af mobile kommunikationsnetværksstandarder af Det Europæiske Standardiseringsinstitut for Telekommunikation, når disse leverer kommunikationstjenester.

(2) De fastsatte krav i dette kapitel finder ikke anvendelse på følgende udstyr:

1) fysisk infrastruktur af kommunikationsnetværket i henhold til § 61², stk. 1, i byggeloven

2) netværkselementer, der ikke er i stand til at behandle signaler eller ikke kræver energi for at fungere

3) strømforsyningsenheder

- 4) klimaanlæg
- 5) terminaludstyr, der ejes eller opbevares af slutbrugeren.

Del 2

Meddelelsespligt

§ 3² Meddelelse om hardware og software, der anvendes i kommunikationsnetværk

Stk. 1. Pr. 1. marts i hvert kalenderår skal en kommunikationsvirksomhed oplyse forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed om den hardware og software, der anvendes i dennes kommunikationsnetværk pr. 1. januar det pågældende år.

Stk. 2. I meddelelsen, til hvilken der henvises i stk. 1, skal kommunikationsvirksomheden oplyse følgende om den anvendte hardware og software i kommunikationsnetværket:

- 1) navn og versionsnummer
 - 2) mængde
 - 3) producentens navn
 - 4) ejerens navn
 - 5) navn på parterne i kontrakten om brugsrettigheder og gyldighedsperioden for brugsrettigheden, hvis ejeren af hardwaren eller softwaren ikke er en kommunikationsvirksomhed
 - 6) funktion i kommunikationsnetværket
 - 7) fysisk anvendelsesområde, som kan angives som en stat, en administrativ enhed, bosættelse, adresseobjekt eller en anden regional præcisering
 - 8) eksistensen eller fraværet af en tilladelse til brug af hardware eller software
 - 9) den generation af standarden for mobile netværk, som hardwaren eller softwaren fungerer med, hvis der er tale om hardware eller software, der bruges i et mobilt netværk
 - 10) en liste over juridiske personer, der ud over kommunikationsvirksomheden har administrativ adgang til hardware eller software, og betingelserne for adgang for hver juridisk person
 - 11) udbydere af vedligeholdelses- og støttetjenester, der bruges i kommunikationsnetværket individuelt af juridiske personer, hvis der er tale om andre personer end dem omhandlet i nr. 4) og 5)
 - 12) præcisering af de dele af meddelelsen, der bør være underlagt adgangsbegrænsninger i henhold til lov om offentlig information.
- (3) Forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed skal fremsende meddelelsen som omhandlet i stk. 1 til sikkerhedsmyndighederne og den statslige myndighed for informationssystemer til orientering.

Del 3

Forpligtelse til en tilladelse til brug

§ 3³ Tilladelse til brug af hardware eller software og ansøgningsproceduren

(1) En kommunikationsvirksomhed skal indsende en ansøgning om brugstilladelse til hardware eller software til forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed inden den planlagte brug af hardwaren eller softwaren.

(2) En kommunikationsvirksomhed skal indsende en ansøgning om brugstilladelse inden for ti arbejdsdage efter udrulningen af hardwaren eller softwaren, hvis den umiddelbare udrulning af hardwaren eller softwaren kræves til forhindring eller forebyggelse af en cyberhændelse i henhold til lov om cybersikkerhed.

(3) I en ansøgning og brugstilladelse skal kommunikationsvirksomheden indsende de oplysninger, der er nævnt i § 3², stk. 2, nr. 1), 3) til 7) og 9) til 11), og skal præcisere de dele af ansøgningen om tilladelse til brug af hardware eller software, der bør være underlagt adgangsbegrænsninger henhold til lov om offentlig information.

(4) En kommunikationsvirksomhed kan udskifte hardware og udføre softwareopdateringer uden at ansøge om tilladelsen til brug af hardware eller software, i hvilken forbindelse navnet eller versionsnummeret på den godkendte hardware eller software i tilladelsen ændres, forudsat at andre oplysninger, der er godkendt i tilladelsen, forbliver uændrede.

§ 3⁴ Behandling og godkendelse af ansøgning om tilladelse til brug af hardware eller software

(1) Forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed videresender en ansøgning om brugstilladelse senest fem arbejdsdage efter modtagelsen til sikkerhedsmyndighederne og den statslige myndighed for informationssystemer, som skal fremkomme med en vurdering.

(2) Hvis en sikkerhedsmyndighed eller den statslige myndighed for informationssystemer vurderer, at hardwaren eller softwaren i et kommunikationsnetværk, der er specificeret i en ansøgning om tilladelse, kan udgøre en fare for den nationale sikkerhed, skal denne fremkomme med en begrundet udtalelse vedrørende ansøgningen om tilladelse inden for 20 arbejdsdage sammen med et forslag til at forhindre brugen af hardware eller software eller pålægge betingelser for dens brug.

(3) Hvis sikkerhedsmyndigheden eller den statslige myndighed for informationssystemer angiver i sin udtalelse, at den specificerede hardware eller software i ansøgningen kan udgøre en fare for den nationale sikkerhed, skal forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed give kommunikationsvirksomheden mulighed for, inden for 20 arbejdsdage, at fremkomme med en udtalelse om, hvorledes afslaget på ansøgningen eller indførelsen af betingelser har indflydelse på kommunikationsvirksomheden og leveringen af kommunikationstjenester, og samtidig fremsætte et forslag om betingelser.

(4) Efter fristen for indgivelse af den anførte udtalelse i stk. 3 skal forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed fremsende kommunikationsvirksomhedens ansøgning sammen med de omtalte udtalelser i stk. 2 og 3 til rådet for cybersikkerhed under sikkerhedskommissionen under republikkens regering (i det følgende

benævnt: rådet for cybersikkerhed)

(5) I forbindelse med godkendelsen skal rådet for cybersikkerhed vurdere, om hardwaren eller softwaren i kommunikationsnetværket, der er specificeret i ansøgningen om brugstilladelse, er højrisikohardware eller -software, eller om brugen af disse kan udgøre en fare for den nationale sikkerhed på grund af tekniske opsætninger eller indstillinger. I tilfælde, hvor hardwaren eller softwaren kan udgøre en fare for den nationale sikkerhed, skal rådet for cybersikkerhed vurdere betingelserne, under hvilke hardwaren eller softwaren kan bruges, og overveje betydningen af at afslå eller indføre betingelser for en tilladelse til brug af hardware eller software for kommunikationsvirksomheden, for kommunikationstjenestens og kommunikationsnetværkets kontinuitet, kommunikationsmarkedet og konkurrencen, samt vurdere brugstilladelsens varighed.

(6) Rådet for cybersikkerhed skal godkende ansøgningen eller give begrundet afslag inden for 30 arbejdsdage efter modtagelse af de materialer, der er specificeret i stk. 4. Om nødvendigt kan rådet for cybersikkerhed udvide godkendelsesfristen med op til 15 arbejdsdage. Forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed skal informeres herom.

§ 3⁵ Præcisering af brugstilladelsens gyldighedsperiode

Ved udskiftning af hardware eller opdatering af software i de anførte tilfælde i § 3³, stk. 4, fortsætter gyldighedsperioden for den tidligere udstedte tilladelse til den udskiftede hardware eller opdaterede software for den nye hardware og software.

§ 3⁶ Frist for tilladelsesproceduren

(1) Forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed skal træffe beslutning om imødekommelse af en ansøgning om brug fra en kommunikationsvirksomhed og om udstedelse af en brugstilladelse inden for 30 arbejdsdage efter modtagelse af en sådan, medmindre den fastlagte procedure i § 3⁴, stk. 3 til 6, er nødvendig.

(2) Hvis § 3⁴, stk. 3 til 6, finder anvendelse på ansøgningen, træffer forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed afgørelse om at imødekomme eller afslå en ansøgning om brugstilladelse og om udstedelse af en brugstilladelse inden for 105 arbejdsdage efter modtagelsen heraf.

Del 4

Revisionsforpligtelse

§ 3⁷ Revisionsforpligtelsens indhold og tilrettelæggelse

(1) Den overensstemmelsesrevision, der skal bestilles af en kommunikationsvirksomhed, kontrollerer, om kommunikationsvirksomheden har opfyldt de forpligtelser, der er pålagt i henhold til § 87³ i lov om elektronisk kommunikation og specificeret i denne forskrift.

(2) For så vidt angår forpligtelsen til at oplyse om hardware og software kontrollerer revisoren, at kommunikationsvirksomheden:

1) har opfyldt meddelelsespligten inden fristens udløb

2) at indholdet af den fremsendte meddelelse svarer til kravene i § 3², stk. 2, og fuldt ud afspejler den hardware og software, som kommunikationsvirksomheden bruger på meddelelsetidspunktet.

(3) For så vidt angår kravet om tilladelse til brug af hardware eller software kontrollerer revisoren, om kommunikationsvirksomheden:

1) har opfyldt tilladelsesforpligtelsen inden for tidsfristen og for hver hardware eller software, der er omfattet af tilladelsesforpligtelsen

2) har indgivet en ansøgning om tilladelse til brug af hardware eller software med indhold, der opfylder kravene i § 3³, stk. 3

3) med rimelighed har påberåbt sig kravene i § 3³, stk. 2, ved forhindring eller direkte forebyggelse af en cyberhændelse

4) med rette har udeladt en ansøgning om tilladelse til brug af hardware eller software i situationer, der er nævnt i § 3³, stk. 4.

(4) Revisoren forelægger resultaterne af de revisioner, der er omhandlet i stk. 2 og 3, for forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed 30 dage efter, at revisionen er udført."

5) Forskriften suppleres med §§ 8¹ og 8² med følgende ordlyd:

"§ 8¹. Gennemførelse af forpligtelsen til at ansøge om en brugstilladelse

(1) En ansøgning om tilladelse til brug af hardware eller software, der blev taget i brug før den 1. februar 2022 eller i perioden fra den 1. februar til den 31. maj 2022, og som omfatter en funktion af 5G-NSA eller højere generation af mobilnetstandarden, skal indgives senest den 1. juni 2022.

(2) De frister, der er fastsat i § 3⁴ og § 3⁶, stk. 2, finder ikke anvendelse på behandlingen af den i stk. 1 omhandlede ansøgning. Forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed behandler ansøgninger om tilladelse til brug af hardware eller software, der indgives på grundlag af stk. 1, senest den 31. december 2022.

§ 8². Gennemførelse af forpligtelsen til at oplyse om hardware og software, der bruges i kommunikationsnetværket

Meddelelsespligten i § 3², stk. 1, skal være opfyldt første gang senest den 1. marts 2023."

§ 2. Ændring af forskrift nr. 129 af 11. december 2015 fra republikkens regering om statutten for sikkerhedskommissionen under republikkens regering

Forskrift nr. 129 af 11. december 2015 fra republikkens regering om statutten for sikkerhedskommissionen under republikkens regering ændres med følgende ordlyd:

1) I forskriftens § 2, stk. 1, ændres "minister for udenrigshandel og informationsteknologi" til "erhvervs- og informationsministeren".

2) Forskriften suppleres med § 7¹ med følgende ordlyd:

§ 7¹. Råd for cybersikkerhed

(1) Rådet for cybersikkerhed arbejder under kommissionen.

(2) Rådet for cybersikkerhed skal:

1) udarbejde retningslinjer for udviklingen af en politik om cybersikkerhed

- 2) indtage standpunkter om planer vedrørende cybersikkerhed
 - 3) sikre, at brugen af den specificerede hardware og software i kommunikationsvirksomhedens ansøgning er i overensstemmelse med statens sikkerhedsinteresser
 - 4) udføre andre opgaver, som det tillægges af kommissionen.
- (3) Under udførelsen af den specificerede opgave i stk. 2, nr. 3), har rådet for cybersikkerhed de rettigheder og forpligtelser, som den administrative myndighed tillægges i loven om administrative procedurer.
- (4) Rådet for cybersikkerhed har en formand og en leder. Arbejdet i rådet for cybersikkerhed forvaltes af lederen.
- (5) Rådet for cybersikkerhed omfatter medlemmer fra følgende ministerier og agenturer:
- 1) Databeskyttelsesinspektoratet
 - 2) Undervisnings- og forskningsministeriet
 - 3) Justitsministeriet
 - 4) Forsvarsforbundet
 - 5) Forsvarsministeriet
 - 6) Den estiske interne sikkerhedstjeneste
 - 7) Forsvarsstyrker
 - 8) Miljøministeriet
 - 9) Kulturministeriet
 - 10) Landbrugsministeriet
 - 11) Økonomi- og kommunikationsministeriet
 - 12) Politi- og grænsepolitirådet
 - 13) Den offentlige anklagemyndighed
 - 14) Finansministeriet
 - 15) Den statslige myndighed for informationssystemer
 - 16) Regeringskontoret
 - 17) Indenrigsministeriet
 - 18) Socialministeriet
 - 19) Forbrugerbeskyttelsesmyndigheden og den tekniske reguleringsmyndighed
 - 20) Det udenlandske efterretningstjeneste
 - 21) Udenrigsministeriet.
- (6) Et stedfortrædende medlem af rådet for cybersikkerhed har rettighederne for det afløste

medlem.

(7) Om nødvendigt tilrettelægges inddragelsen af andre personer i arbejdet i rådet for cybersikkerhed af direktøren for rådet for cybersikkerhed.

(8) Rådet for cybersikkerhed er beslutningsdygtigt, hvis mindst to tredjedele af rådets medlemmer, der har stemmeret, deltager i mødet. Ved udførelsen af den opgave, der er nævnt i stk. 2, nr. 3), er rådet for cybersikkerhed beslutningsdygtigt, hvis medlemmer af rådet for cybersikkerhed fra regeringskontoret, forsvarsministeriet, økonomi- og kommunikationsministeriet, indenrigsministeriet og udenrigsministeriet deltager i mødet.

(9) Rådet for cybersikkerheds afgørelser træffes ved et flertal af stemmerne fra de medlemmer, der har stemmeret og er til stede ved mødet. Regeringskontoret og ministerierne har stemmeret. Hvert ministerium og regeringskontoret har én stemme. Ved stemmelighed er rådet for cybersikkerheds mødeformands stemme, eller ved dennes fravær, lederens stemme, afgørende.

(10) Regeringskontoret, forsvarsministeriet, økonomi- og kommunikationsministeriet, indenrigsministeriet og udenrigsministeriet har ved udførelsen af den opgave, der er nævnt i stk. 2, nr. 3), stemmeret.

(11) Rådet for cybersikkerheds procedureregler skal godkendes af udvalget.

(12) De procedureregler, der er nævnt i stk. 11, fastsætter følgende:

- 1) formand og leder af rådet for cybersikkerhed
- 2) medlemmer fra de i stk. 5 nævnte ministerier og agenturer i kraft af deres stilling
- 3) udskiftning af medlemmer, formand og leder af rådet for cybersikkerhed
- 4) andre organisatoriske krav."

§ 3. Forskriftens ikrafttræden

Nærværende forskrift træder i kraft den 1. februar 2022.

Jaak Aab

Ministeren for offentlig forvaltning i hvervet som premierminister

Andres Sutt

Ministeren for erhverv og informationsteknologi

Taimar Peterkop

Statssekretær