Innehållsförteckning

1. Utdrag ur lagen om ändring av lagen om elektronisk kommunikation, byggnadslagen och lagen om statliga avgifter – sida 2.
   Förklaring: i detta avsnitt beskrivs de rättsliga bestämmelserna om genomförandet av 5G-verktygslådan. Bestämmelserna genom vilka Europaparlamentets och rådets direktiv (EU) 2018/1972 genomförs har strukits.
   Den fullständiga texten till lagen om ändring av lagen om elektronisk kommunikation, byggnadslagen och lagen om statliga avgifter finns tillgänglig på: https://www.riigiteataja.ee/akt/115122021001.
   Den gällande fullständiga texten till lagen om elektronisk kommunikation finns på: https://www.riigiteataja.ee/akt/122102021015?leiaKehtiv.

2. Estlands regeringsförordning nr 119 av den 16 december 2021 om ändring av Estlands regeringsförordning nr 140 av den 22 juni 2006 om krav för tillhandahållande av kommunikationstjänster och tekniska krav för kommunikationsnät och av Estlands regeringsförordning nr 129 av den 11 december 2015 om stadgar för regeringens säkerhetskommitté – s. 5.

1. Utdrag ur lagen om ändring av lagen om elektronisk kommunikation, byggnadslagen och lagen om statliga avgifter.

1 §. Ändring av lagen om elektronisk kommunikation

Lagen om elektronisk kommunikation ska ändras på följande sätt:

111) underavsnitt 87.2^1 och 87.2^2 ska upphävas.

118) I lagen införs avsnitt 87^3–87^5 med följande lydelse:

”87^3 §. Krav för kommunikationsnät och kommunikationstjänster för att säkerställa den nationella säkerheten

(1) Hårdvara och programvara som används för tillhandahållande av kommunikationstjänster i ett kommunikationsnät får inte utgöra en risk för den nationella säkerheten.

(2) Hårdvara och programvara som används för tillhandahållande av kommunikationstjänster i ett kommunikationsnät kan utgöra en risk för den nationella säkerheten till följd av
1) en hög risk som följer av producenten eller leverantören av en underhålls- eller stödtjänst (nedan kallad *hårdvara eller programvara med hög risk*),
2) en risk som följer av hårdvarans eller programvarans tekniska egenskaper eller konfiguration.

3)) Vid bedömning av hårdvara eller programvara med hög risk beaktas bland annat information om huruvida
1) producenten eller leverantören av underhålls- eller supporttjänster har sitt säte eller huvudkontor i ett land (nedan kallat *hemvistland*) som inte är medlem i Europeiska unionen, Nordatlantiska fördragsorganisationen (nedan kallad *Nato*) eller Organisationen för ekonomiskt samarbete och utveckling (nedan kallad *OECD*),
2) den demokratiska rättsstatsprincipen inte följs eller de mänskliga rättigheterna inte respekteras i det där producenten eller leverantören av underhålls- eller supporttjänster har sin hemvist,
3) immateriella rättigheter, personuppgifter eller affärshemligheter för personer från andra länder inte skyddas i det land där producenten eller leverantören av underhålls- eller stödtjänster har sin hemvist,
4) det land där producenten eller leverantören av underhålls- eller supporttjänster har sin hemvist uppvisar aggressiva beteenden i cyberrymden,
5) it-angrepp har tillskrivits det land där producenten eller leverantören av underhålls- eller supporttjänster har sin hemvist av medlemsstaterna i Europeiska unionen, Nato eller OECD,
6) producenten eller leverantören av underhålls- eller supporttjänster är underkastad regeringen eller den statliga myndigheten i dennes hemvistland eller ett annat främmande land utan oberoende rättslig kontroll,
7) det land där producenten eller leverantören av underhålls- eller supporttjänster har hemvist eller ett annat främmande land får ålägga denne att agera på ett sätt som utgör en risk för Estlands nationella säkerhet,
8) den ekonomiska verksamhet som bedrivs av producenten eller leverantören av underhålls- eller supporttjänster inte grundas på marknadsbaserad konkurrens eller om inga lämpliga villkor har skapats för detta i hemvistlandet,
9) ägarstrukturen, organisationsstrukturen eller förvaltningsstrukturen hos producenten eller leverantören av underhålls- eller supporttjänster inte är transparent,

10) finansieringen av producenten eller leverantören av underhålls- eller supporttjänster inte är transparent,
11) de produkter eller tjänster som tillhandahålls av producenten eller leverantören av underhålls- eller supporttjänster omfattar sårbarheter och lämpliga säkerhetsåtgärder inte har vidtagits för att undanröja dessa,
12) producenten eller leverantören av underhålls- eller supporttjänster inte kan säkerställa fortsatta leveranser av produkter eller tjänster, undantaget till följd av force majeure.

(4) För att säkerställa nationell säkerhet är kommunikationsföretaget skyldigt att meddela myndigheten för konsumentskydd och tekniska föreskrifter om vilken hårdvara och programvara som används i kommunikationsnätet.

(5) Omfattningen av den anmälningsskyldighet som anges i underavsnitt 4 i detta avsnitt och de särskilda kraven, villkoren för fullgörande av skyldigheten och anmälningsförfarandet fastställs i en förordning från Estlands regering.

(6) För att säkerställa den nationella säkerheten är ett kommunikationsföretag skyldigt att ansöka om användningstillstånd för hårdvara eller programvara i ett kommunikationsnät (nedan kallat *användningstillstånd för hårdvara eller programvara*) från myndigheten för konsumentskydd och tekniska föreskrifter.

(7) Omfattningen av skyldigheten att ansöka om användningstillstånd för hårdvara eller programvara, de särskilda kraven, tidsfristen och tillvägagångssättet för förfarandet och specifikationerna för användningstillståndets giltighetstid fastställs i en förordning från Estlands regering.

(8) Vid utfärdandet av de föreskrifter som anges i underavsnitten 5 och 7 i denna lag beaktar Estlands regering kommunikationsnätets betydelse, dess hårdvara eller programvara och kommunikationstjänster som tillhandahålls i nätet samt de potentiella risker som detta medför för den nationella säkerheten.

87[4] §. Förfaranden för användningstillstånd för hårdvara eller programvara

(1) Efter att ha mottagit en ansökan om användningstillstånd för hårdvara eller programvara ber myndigheten för konsumentskydd och tekniska föreskrifter om yttranden från säkerhetsmyndigheter och informationssystemmyndigheten om huruvida den hårdvara eller programvara som anges i kommunikationsföretagets ansökan om användningstillstånd för hårdvara eller programvara utgör en risk för den nationella säkerheten. Om hårdvaran eller programvaran kan utgöra en risk för den nationella säkerheten enligt det yttrande som mottagits begär myndigheten för konsumentskydd och tekniska föreskrifter ett godkännande från den myndighet som anges i stadgarna för Republiken Estlands säkerhetskommitté (nedan kallad *den administrativa myndigheten*) innan kommunikationsföretagets ansökan om användningstillstånd för hårdvara eller programvara avgörs.

(2) I det godkännandeförfarande som anges i underavsnitt 1 i detta avsnitt bedömer den administrativa myndigheten om användningen av den hårdvara eller programvara som anges i ansökan om användningstillstånd för hårdvara eller programvara utgör en risk för den nationella säkerheten. I godkännandeförfarandet får den administrativa myndigheten inlämna förslag om förbud att använda den hårdvara eller programvara som anges i ansökan om användningstillstånd för hårdvara eller programvara eller om fastställande av villkor för dess användning. Villkoren för användning av hårdvara eller programvara kan bland annat omfatta en tidsgräns för användning, användning i vissa delar eller funktioner eller med viss

konfiguration av kommunikationsnätet.

(3) Med hänsyn till bestämmelserna i underavsnitten 1 och 2 i detta avsnitt ska myndigheten för konsumentskydd och tekniska föreskrifter besluta om godkännande, villkorat godkännande eller avslag på ansökan om användningstillstånd för hårdvara eller programvara.

(4) Om en hårdvara eller programvara inte utgör en risk för den nationella säkerheten beviljas tillstånd för användning för åtta år. Om en hårdvara eller programvara utgör en risk för den nationella säkerheten beviljas inget användningstillstånd eller så beviljas ett villkorat tillstånd för användning.

87^5 §. Revision

1) För kommunikationsföretag som har ålagts skyldigheter med grund i 87^3 § i denna lag föreskrivs en regelefterlevnadsrevision av verksamheten minst vart tredje år efter det att skyldigheten ålades, för bedömning i revisionsberättelsen av huruvida kommunikationsföretaget har fullgjort de skyldigheter som de ålagts med grund i samma avsnitt.

2) Den person som utför revisionen ska vara en oberoende revisor som innehar ett certifierat intyg för informationssystemrevision från ISACA eller liknande intyg.

3) Den person som utför revisionen överlämnar revisionen till myndigheten för konsumentskydd och tekniska föreskrifter.

4) Kostnaderna för att genomföra revisionen täcks av kommunikationsföretaget.

5) Innehållet i den revisionsskyldighet som anges i underavsnitt 1 i detta avsnitt samt tidpunkten och förfarandet för inlämnande av revisionen fastställs i en förordning från Estlands regering.”

152) I lagen införs avsnitt 170^3 med följande lydelse:

”**170^3 §. Åsidosättande av skyldigheter som åläggs med hänsyn till den nationella säkerheten**

(1) Åsidosättandet av de skyldigheter som åläggs med grund i 87^3 § eller 87^5 § i denna lag är straffbart med böter på upp till 300 bötesenheter.

(2) Samma gärning, om den begås av en juridisk person, är belagd med böter på upp till 50 000 euro.”

156) I lagen införs avsnitt 196^3–196^5 med följande lydelse:

196^5 §. Genomförande av 87^3 § och 87^4 § i denna lag

(1) Skyldigheten att ansöka om användningstillstånd för hårdvara eller programvara enligt 87^3.6 § i denna lag ska tillämpas på hårdvara eller programvara som tagits i bruk före den 1 februari 2022 om en funktion av 5G som inte är fristående (nedan kallad *5G NSA*) eller om en nyare generations standard för kommunikation via mobilnät har eller skulle användas i hårdvaran eller programvaran.

(2) Hårdvara eller programvara med hög risk i vilken en funktion av 5G NSA eller en nyare generations standard för kommunikation via mobilnät används eller skulle användas och som inte har en kritisk funktion får användas på grundval av ett användningstillstånd till och med den 31 december 2025. Användningstillstånd utfärdas inte för hårdvara eller programvara med

hög risk som avses i första meningen efter den 31 december 2025. Tidsfristen för inlämnande av ansökningar om det användningstillstånd för hårdvara eller programvara med hög risk som avses i första meningen fastställs i den förordning som anges i 87^3.7 § i denna lag.

(3) Den hårdvara eller programvara som inte har en funktion av 5G NSA eller en nyare generations standard för kommunikation via mobilnät eller en kritisk funktion får användas till och med den 31 december 2029 utan ansökan om användningstillstånd enligt 87^3.6 § i denna lag.

(4) Om den hårdvara eller programvara som avses i underavsnitt 3 i detta avsnitt är avsedd att användas efter den 31 december 2029 ska en ansökan om användningstillstånd lämnas in senast den 1 juli 2029. Användningstillstånd utfärdas inte för hårdvara eller programvara med hög risk som avses i första meningen efter den 31 december 2029.

(5) Följande utgör kritiska funktioner hos hårdvara och programvara: 1) Stomnätets funktion i enlighet med standarderna från Europeiska institutet för telekommunikationsstandarder, oavsett var i kommunikationsnätet funktionen finns. 2) Den funktion som syftar till att göra det möjligt för säkerhetsmyndigheter och övervakningsorgan att bedriva övervakningsverksamhet eller begränsa rätten till konfidentialitet för meddelanden i de fall som föreskrivs i lag.”

2. Estlands regeringsförordning nr 119 av den 16 december 2021 om ändring av Estlands regeringsförordning nr 140 av den 22 juni 2006 om krav för tillhandahållande av kommunikationstjänster och tekniska krav för kommunikationsnät och Estlands regeringsförordning nr 129 av den 11 december 2015 om stadgar för regeringens säkerhetskommitté.

Utfärdande organ: ESTLANDS REGERING

Typ: förordning

Typ av text: utkast

Ikraftträdande: den 1 februari 2022

Uppgift om offentliggörande: RT I, 21.12.2021, 1

Ändring av Estlands regeringsförordning nr 140 av den 22 juni 2006 om krav för tillhandahållande av kommunikationstjänster och tekniska krav för kommunikationsnät och Estlands regeringsförordning nr 129 av den 11 december 2015 om stadgar för regeringens säkerhetskommitté

Antagen den 16 december 2021, nr 119

Förordningen är fastställd på grundval av 87.2 §, 87^3.5 §, 87^3.7 § och 87^5.5 i lagen om elektronisk kommunikation och 4.2 § i lagen om nationellt försvaret.

1 §. Ändring av förordning nr 140 från Republikens regering av den 22 juni 2006 om krav för tillhandahållande av kommunikationstjänster och tekniska krav för kommunikationsnät

Följande ändringar ska göras i förordning nr 140 från Republikens regering av den 22 juni 2006 om krav för tillhandahållande av kommunikationstjänster och tekniska krav för kommunikationsnät:

1) I 2.1 §, 3.4.1 § och 6.1 § ingressen till förordningen ska orden ”Lagen om elektronisk kommunikation” ersättas med ”lagen om elektronisk kommunikation”.

2) I inledningen till förordningen införs orden ”87^{3}.5 §, 87^{3}.7§ och 87^{5}.5” efter orden ”underavsnitt 2”.

3) Avsnitt 1 ska ha följande lydelse:

”I denna förordning fastställs följande:

1) De krav för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster (nedan kallade *kommunikationstjänster*) som följer av de syften som anges i 87.2.1 §, 87.2.3 § och 87.2.4 § i lagen om elektronisk kommunikation.

2) Tekniska och nationella säkerhetskrav för offentliga elektroniska kommunikationsnät (nedan kallade *kommunikationsnät*).

3) En skyldighet att anmäla den hårdvara och programvara som används i kommunikationsnätet, innehållet i och förfarandet för ansökan om användningstillstånd samt innehållet i och förfarandet för en revisionsskyldighet.”

4) I förordningen införs kapitel 2^{1} med följande lydelse:

”Kapitel 21.

KRAV FÖR KOMMUNIKATIONSTJÄNSTER OCH KOMMUNIKATIONSNÄT FÖR ATT SÄKERSTÄLLA DEN NATIONELLA SÄKERHETEN

Del 1

Allmänna bestämmelser

3^{1} § Kravens tillämpningsområde

(1) Kraven som fastställs i detta kapitel gäller för kommunikationsföretag som tillhandahåller en nödvändig tjänst i enlighet med 87.4 § i lagen om elektronisk kommunikation eller som tillämpar standarderna för 5G som inte är fristående (nedan kallad *5G NSA*) eller högre generationers mobilnät från Europeiska institutet för telekommunikationsstandarder vid tillhandahållandet av kommunikationstjänster.

(2) De krav som fastställs i detta kapitel gäller inte för följande utrustning:

1) Fysisk infrastruktur i ett kommunikationsnät i den mening som avses i 61^{2}.1 § i byggnadslagen.

2) Nätkomponenter som inte kan behandla signaler eller inte förbrukar energi i samband med drift.

3) Strömförsörjningsenheter.

4) Luftkonditioneringsenheter.

5) Terminalutrustning som ägs eller innehas av slutanvändaren.

Del 2

Rapporteringsskyldighet

3[2] § Anmälan om hårdvara och programvara som används i kommunikationsnätet

1) Senast den 1 mars varje kalenderår ska kommunikationsföretaget meddela myndigheten för konsumentskydd och tekniska föreskrifter om vilken hårdvara och programvara som används i dess kommunikationsnät från om med den 1 januari samma år.

2) I anmälan som anges i punkt 1 ska kommunikationsföretaget tillhandahålla följande information om den använda hårdvaran och programvaran i kommunikationsnätet:

1. Beteckning och versionsnummer.

2. Mängd.

3. Producentens namn.

4. Ägarens namn.

5. Namnen på parterna i licensavtalet och giltighetstiden för licensen, om kommunikationsföretaget inte äger hårdvaran eller programvaran.

6. Funktion i kommunikationsnätet.

7. Fysiskt område för användning, vilket kan anges som en stat, administrativ enhet, bostadsområde, adressobjekt eller annan områdesspecifik uppgift.

8. Förekomsten eller avsaknaden av ett användningstillstånd för hårdvara eller programvara.

9. När det gäller hårdvara eller programvara som används i ett mobilnät, den generation av standard för mobilnät som hårdvaran eller programvaran fungerar med.

10) En förteckning över de juridiska personer som utöver kommunikationsföretaget har administrativ tillgång till hårdvaran eller programvaran, och villkoren för tillgång för varje juridisk person.

11) Leverantörer som tillhandahåller service- och supporttjänster för hårdvara och programvara i kommunikationsnätet, angivet per juridisk person om dessa skiljer sig från de personer som avses i klausulerna 4 och 5.

12) Specificering av de delar av anmälan som bör omfattas av tillgångsbegränsningar enligt lagen om offentlig information.

(3) Myndigheten för konsumentskydd och tekniska föreskrifter ska översända den anmälan som avses i underavsnitt 1 till säkerhetsmyndigheterna och statens informationssystemmyndighet i upplysningssyfte.

Del 3

Krav på användningstillstånd

3[3] § Användningstillstånd för hårdvara eller programvara och ansökningsförfarandet

(1) Ett kommunikationsföretag ska lämna in en tillståndsansökan för användning av hårdvara eller programvara till myndigheten för konsumentskydd och tekniska föreskrifter innan denna tas i avsett bruk.

(2) Ett kommunikationsföretag ska lämna in en ansökan om användningstillstånd senast tio arbetsdagar efter det att hårdvaran eller programvaran har tagits i bruk om denna behöver tas i bruk omedelbart för att undanröja eller förhindra en it-incident i den mening som avses i lagen om cybersäkerhet.

(3) I ansökan om användningstillstånd ska kommunikationsföretaget ange den information som avses i klausulerna 1, 3–7 och 9–11 i 3[2].2 § och ange vilka delar av ansökan om användningstillstånd för hårdvara eller programvara som skulle omfattas av tillgångsbegränsningar i enlighet med lagen om offentlig information.

(4) Kommunikationsföretag behöver inte ansöka om ett användningstillstånd för hårdvara eller programvara för att byta ut hårdvara eller uppdatera programvara som innebär att beteckningen eller versionsnumret för den godkända hårdvaran eller programvaran i tillståndet ändras, förutsatt att övriga uppgifter som godkänts i tillståndet förblir oförändrade.

3[4] § Behandling och godkännande av ansökan om användningstillstånd för hårdvara eller programvara

(1) Myndigheten för konsumentskydd och tekniska föreskrifter ska översända en ansökan om användningstillstånd till säkerhetsmyndigheterna och statens informationssystemmyndighet inom fem arbetsdagar från mottagandet så att de kan ta ställning till ansökan och avge ett yttrande.

(2) Om en säkerhetsmyndighet eller statens informationssystemmyndighet finner att den i tillståndsansökan angivna hårdvaran eller programvaran i kommunikationsnätet kan äventyra den nationella säkerheten ska myndigheten inom 20 arbetsdagar lämna in ett motiverat yttrande om tillståndsansökan tillsammans med ett förslag om förbud av användning av hårdvaran eller programvaran eller om införande av villkor för dess användning.

(3) Om säkerhetsmyndigheten eller statens informationssystemmyndighet konstaterar i ett yttrande att den i ansökan angivna hårdvaran eller programvaran kan äventyra den nationella säkerheten ska myndigheten för konsumentskydd och tekniska föreskrifter ge kommunikationsföretaget möjlighet att inom 20 arbetsdagar inkomma med ett yttrande om hur avslaget på ansökan eller införandet av villkor påverkar kommunikationsföretaget och tillhandahållandet av kommunikationstjänsterna samt ett villkorsförslag.

(4) Efter det att tidsfristen för att avge det yttrande som föreskrivs i underavsnitt 3 har löpt ut ska myndigheten för konsumentskydd och tekniska föreskrifter lämna in kommunikationsföretagets ansökan tillsammans med de yttranden som anges i underavsnitten 2 och 3 till regeringens säkerhetskommittés cybersäkerhetsråd (nedan kallat *cybersäkerhetsrådet*).

(5) I samband med godkännandet ska cybersäkerhetsrådet bedöma huruvida den hårdvara eller programvara som ska användas i kommunikationsnätet, och som har angetts i ansökan om

användningstillstånd, utgör en hög risk eller om användningen kan äventyra den nationella säkerheten till följd av tekniska funktioner eller inställningar. Om hårdvaran eller programvaran kan utgöra ett hot mot nationell säkerhet ska cybersäkerhetsrådet bedöma de förutsättningar under vilka hårdvaran eller programvaran får användas liksom hur kommunikationsföretag, kontinuiteten hos kommunikationstjänster och kommunikationsnät, kommunikationsmarknaden och konkurrensen kan komma att påverkas vid avvisande eller om vissa villkor för användningstillstånd för hårdvara eller programvara införs. Användningstillståndets giltighetstid ska likaså utvärderas.

(6) Cybersäkerhetsrådet ska godkänna ansökan eller avslå den om rimliga tvivel föreligger inom 30 arbetsdagar från mottagandet av det material som anges i underavsnitt 4. Vid behov kan cybersäkerhetsrådet förlänga godkännandeperioden med upp till 15 arbetsdagar. Myndigheten för konsumentskydd och tekniska föreskrifter ska i så fall underrättas om detta.

3^5 § Angivelse av giltighetstiden för användningstillstånd

Vid ersättning av hårdvara eller uppdatering av programvara i det fall som anges i 3^3.4 § ska giltighetsperioden för det tidigare beviljade tillståndet för den utbytta hårdvaran eller uppdaterade programvaran fortsätta att gälla för den nya hårdvaran eller programvaran.

3^6 § Tidsfrist för godkännandeförfarandet

(1) Myndigheten för konsumentskydd och tekniska föreskrifter ska fatta ett beslut om godkännande eller avslag av ett kommunikationsföretags ansökan och utfärdande av användningstillstånd inom 30 arbetsdagar från mottagandet av ansökan, såvida inte det förfarande som anges i 3^4.3–3^4.6 § behöver tillämpas.

(2) Om 3^4.3–3^4.6 § är tillämplig på ansökan ska myndigheten för konsumentskydd och tekniska föreskrifter besluta om ansökan om användningstillstånd ska godkännas eller avslås och om utfärdande av användningstillstånd inom 105 arbetsdagar efter mottagandet av denna.

Del 4

Revisionsskyldighet

3^7 § Revisionsskyldighetens innehåll och organisation

(1) Den regelefterlevnadsrevision som ska beställas av ett kommunikationsföretag ska kontrollera huruvida kommunikationsföretaget har uppfyllt de skyldigheter som åläggs genom 87^3 § i lagen om elektronisk kommunikation och som specificeras i denna förordning.

(2) När det gäller skyldigheten att anmäla hårdvara och programvara ska revisorn kontrollera att

1) kommunikationsföretaget har uppfyllt anmälningsskyldigheten inom tidsfristen,

2) innehållet i kommunikationsföretagets inlämnade anmälan motsvarar kraven i 3^2.2 § och återspeglar till fullo den hårdvara och programvara som kommunikationsföretaget använde vid tidpunkten för anmälan.

(3) När det gäller kravet på användningstillstånd för hårdvara eller programvara ska revisorn kontrollera huruvida kommunikationsföretaget

1) har uppfyllt tillståndskravet inom tidsfristen och för varje hårdvara eller programvara som omfattas av tillståndskravet,

2) har lämnat in en ansökan om användningstillstånd för hårdvara eller programvara, vars innehåll överensstämmer med kraven i 3^3.3 §,

3) rimligen har förlitat sig på kraven i 3^3.2 § för att undanröja eller förhindra it-incidenter,

4) med rätta har utelämnat en ansökan om användningstillstånd för hårdvara eller programvara i situationer som avses i 3^3.4 §.

(4) Revisorn ska överlämna resultaten av de revisioner som anges i underavsnitten 2 och 3 till myndigheten för konsumentskydd och tekniska föreskrifter senast 30 dagar efter det att revisionen har utförts.”

5) I lagen införs 8^1 § och 8^2 § med följande lydelse:

”**8^1 §. Införande av skyldigheten att ansöka om användningstillstånd**

(1) En ansökan om användningstillstånd för hårdvara eller programvara som togs i bruk före den 1 februari 2022 eller mellan den 1 februari och den 31 maj 2022 och som omfattar en funktion av 5G NSA eller högre generationers standard för mobilnät ska lämnas in senast den 1 juni 2022.

(2) De tidsfrister som anges i 3^4 § och 3^6.2 § ska inte tillämpas på behandlingen av den ansökan som avses i underavsnitt 1. Myndigheten för konsumentskydd och tekniska föreskrifter ska senast den 31 december 2022 besluta om ansökningar om användningstillstånd för hårdvara eller programvara som lämnats in på grundval av underavsnitt 1.

8^2 §. Införande av skyldigheten att anmäla hårdvara och programvara som används i kommunikationsnätet

Den anmälningsskyldighet som avses i 3^2.1 § ska uppfyllas för första gången senast den 1 mars 2023.”

2 §. Ändring av förordning nr 129 från Republikens regering av den 11 december 2015 om stadgar för regeringens säkerhetskommitté

Förordning nr 129 från Estlands regering av den 11 december 2015 om stadgar för regeringens säkerhetskommitté ska ändras på följande sätt:

1) I 2.1 § i förordningen ska orden ”ministern för utrikeshandel och informationsteknik” ersättas med orden ”ministern för näringsliv och informationsteknik”.

2) I lagen införs 7^1 § med följande lydelse:

7^1 §. Cybersäkerhetsrådet

(1) Cybersäkerhetsrådet verkar vid kommittén.

(2) Cybersäkerhetsrådet ska

1) tillhandahålla riktlinjer för utvecklingen av it-säkerhetspolitik,

2) uttala sig om planer som gäller it-säkerhet,

3) säkerställa att användningen av hårdvara och programvara som angetts i kommunikationsföretagets ansökan överensstämmer med statens säkerhetsintressen,

4) utföra andra uppgifter som tilldelats av kommittén.

(3) Vid utförande av den uppgift som anges i punkt 2.3 har cybersäkerhetsrådet de rättigheter och skyldigheter som fastställts för en administrativ myndighet i lagen om förvaltningsförfaranden.

(4) Cybersäkerhetsrådet har en ordförande och en chef. Cybersäkerhetsrådets arbete leds av chefen.

(5) I cybersäkerhetsrådet ingår ledamöter från följande ministerier och organ:

1) Dataskyddsinspektionen.

2) Ministeriet för utbildning och forskning.

3) Justitieministeriet.

4) Hemvärnet.

5) Försvarsministeriet.

6) Estlands inre säkerhetstjänst.

7) Försvarsmakten.

8) Miljöministeriet.

9) Kulturministeriet.

10) Landsbygdsministeriet.

11) Finans- och kommunikationsministeriet.

12) Polis- och gränsbevakningsnämnden.

13) Åklagarmyndigheten.

14) Finansministeriet.

15) Statens informationssystemmyndighet.

16) Regeringskansliet.

17) Inrikesministeriet.

18) Socialministeriet.

19) Myndigheten för konsumentskydd och tekniska föreskrifter.

20) Myndigheten för utrikesunderrättelse.

21) Utrikesministeriet.

(6) En suppleant i cybersäkerhetsrådet ska ha samma rättigheter som den ersatta ledamotens.

(7) Vid behov ska andra personers deltagande i cybersäkerhetsrådets arbete organiseras av chefen för cybersäkerhetsrådet.

(8) Cybersäkerhetsrådet är beslutfört om minst två tredjedelar av rådets ledamöter med rösträtt deltar i sammanträdet. Vid utförandet av den uppgift som anges i underavsnitt 2.3 ska cybersäkerhetsrådet vara beslutsfört om cybersäkerhetsrådets ledamöter från regeringskansliet,

försvarsministeriet, finans- och kommunikationsministeriet, inrikesministeriet och utrikesministeriet deltar i sammanträdet.

(9) Cybersäkerhetsrådets beslut ska fattas genom majoritetsröstning av de ledamöter med rösträtt som närvarar vid mötet. Regeringskansliet och ministerierna har rösträtt. Varje ministerium och regeringskansliet har varsin röst. Vid lika röstetal ska ordföranden för cybersäkerhetsrådets, eller vid dennes frånvaro chefens, röst vara utslagsgivande.

(10) Vid utförandet av den uppgift som anges i underavsnitt 2.3 ska regeringskansliet, försvarsministeriet, finans- och kommunikationsministeriet, inrikesministeriet och utrikesministeriet ha rösträtt.

(11) Cybersäkerhetsrådets arbetsordning ska godkännas av kommittén.

(12) I den arbetsordning som avses i underavsnitt 11 ska följande fastställas:

1) Cybersäkerhetsrådets ordförande och chef.

2) Ledamöter från de ministerier och myndigheter som avses i underavsnitt 5 genom sina befattningar.

3) Suppleanter för cybersäkerhetsrådets ledamöter, ordförande och chef.

4) Andra organisatoriska krav.”

3 §. Förordningens ikraftträdande

Denna förordning träder i kraft den 1 februari 2022.

Jaak Aab

Ministern för offentlig förvaltning i egenskap av premiärminister

Andres Sutt

Ministern för näringsliv och informationsteknik

Taimar Peterkop

Statssekreterare