Cuprins

1. Extrase din Legea de modificare a Legii privind comunicațiile electronice, a Codului construcțiilor și a Legii privind taxele de stat.

Articolul 1. Modificarea Legii privind comunicațiile electronice

Următoarele modificări sunt aduse Legii privind comunicațiile electronice:

111) Articolul 87 alineatele ($2^{1)}$ și ($2^{2)}$ se abrogă;

118) Legea se completează cu articolele 87^3-87^5 care au formularea următoare:

„**Articolul 87^3. Cerințe privind rețelele și serviciile de comunicații pentru asigurarea securității naționale**

(1) Hardware-ul și software-ul utilizate pentru furnizarea de servicii de comunicații într-o rețea de comunicații nu trebuie să reprezinte un risc pentru securitatea națională.

(2) Hardware-ul și software-ul utilizate pentru furnizarea de servicii de comunicații într-o rețea de comunicații pot prezenta un risc pentru securitatea națională ca urmare a:
1) unui risc ridicat provenit de la producătorul sau furnizorul său de servicii de întreținere sau de asistență (denumit în continuare „hardware sau software cu risc ridicat”);
2) unui risc care decurge din caracteristicile tehnice sau configurația hardware-ului sau a software-ului.

3)) La evaluarea hardware-ului sau a software-ului cu risc ridicat, se ține seama, printre altele, de informații cu privire la faptul dacă:
1) producătorul sau furnizorul de servicii de întreținere sau de asistență are sediul social sau sediul central într-o țară (denumită în continuare „țara de domiciliu”), care nu este un stat membru al Uniunii Europene, al Organizației Tratatului Atlanticului de Nord (denumită în continuare „NATO”) sau al Organizației pentru Cooperare și Dezvoltare Economică (denumită în continuare „OCDE”);
2) principiile statului de drept democratic nu sunt respectate sau drepturile omului nu sunt respectate în țara de domiciliu a producătorului sau a prestatorului de servicii de întreținere sau de sprijin;
3) proprietatea intelectuală, datele cu caracter personal sau secretele comerciale ale persoanelor din alte țări nu sunt protejate în țara de domiciliu a producătorului sau a furnizorului de servicii de întreținere sau de asistență;
4) țara de domiciliu a producătorului sau a furnizorului de servicii de întreținere sau de asistență prezintă un comportament agresiv în spațiul cibernetic;
5) statele membre ale Uniunii Europene, NATO sau OCDE au atribuit atacuri cibernetice țării de domiciliu a producătorului sau a furnizorului de servicii de întreținere sau de asistență;
6) producătorul sau furnizorul de servicii de întreținere sau de asistență este supus guvernului sau autorității de stat a țării de domiciliu sau a altei țări străine care nu are un control judiciar independent;
7) țara de domiciliu a producătorului sau a furnizorului de servicii de întreținere sau de sprijin sau a unei alte țări străine o poate obliga să acționeze într-un mod care prezintă un risc pentru securitatea națională a Estoniei;
8) activitățile economice ale producătorului sau ale furnizorului de servicii de întreținere sau de sprijin nu se bazează pe o concurență bazată pe piață sau nu au fost create condiții adecvate pentru aceasta în țara de domiciliu;
9) structura de proprietate, structura organizatorică sau structura de conducere a

producătorului sau a furnizorului de servicii de întreținere sau de asistență nu este transparentă;
10) finanțarea producătorului sau a furnizorului de servicii de întreținere sau de asistență nu este transparentă;
11) produsele sau serviciile producătorului sau ale furnizorului de servicii de întreținere sau de asistență includ vulnerabilități și nu au fost puse în aplicare măsuri de securitate adecvate pentru a le elimina;
12) producătorul sau furnizorul de servicii de întreținere sau de asistență nu este în măsură să asigure continuarea livrărilor de produse sau servicii, cu excepția cazurilor de forță majoră.

(4) Pentru a asigura securitatea națională, o întreprindere de comunicații este obligată să notifice Autoritatea pentru protecția consumatorilor și reglementare tehnică cu privire la hardware și software utilizate în rețeaua de comunicații.

(5) Întinderea obligației de notificare specificate la alineatul (4) de la prezentul articol, precum și cerințele specifice, termenul de respectare a obligației și procedura de notificare se stabilesc printr-un regulament al Guvernului Republicii.

(6) Pentru a asigura securitatea națională, o întreprindere de comunicații este obligată să solicite o autorizație de utilizare a hardware-ului sau a software-ului unei rețele de comunicații (denumită în continuare „autorizație de utilizare a hardware-ului sau software-ului") din partea Autorității pentru protecția consumatorilor și reglementare tehnică.

(7) Întinderea obligației de a solicita o autorizație de utilizare a hardware-ului sau a software-ului, cerințele specifice, termenul și procedura procesului, precum și specificațiile privind durata autorizației de utilizare sunt stabilite printr-un regulament al Guvernului Republicii.

(8) La emiterea reglementărilor specificate la alineatele (5) și (7) din prezenta lege, Guvernul Republicii ține seama de importanța rețelei de comunicații, a hardware-ului sau a serviciilor sale software și de comunicații furnizate în rețea, precum și de riscurile potențiale care decurg din aceasta pentru securitatea națională.

Articolul 87[4]. Proceduri de autorizare pentru utilizarea hardware-ului sau a software-ului

(1) La primirea unei cereri de autorizare de utilizare a hardware-ului sau a software-ului, Autoritatea pentru protecția consumatorilor și de reglementare tehnică solicită avizul autorităților de securitate și al autorității sistemului informațional cu privire la măsura în care hardware-ul sau software-ul specificat în cererea întreprinderii de comunicații pentru autorizația de utilizare a hardware-ului sau a software-ului prezintă un risc pentru securitatea națională. În cazul în care hardware-ul sau software-ul poate prezenta un risc pentru securitatea națională în conformitate cu avizul primit, Autoritatea pentru protecția consumatorilor și reglementare tehnică solicită aprobarea autorității menționate în statutul Comitetului de securitate al Republicii Estonia (denumit în continuare „autoritatea administrativă") înainte de soluționarea cererii întreprinderii de comunicații pentru autorizarea utilizării hardware-ului sau a software-ului.

(2) În procesul de aprobare specificat în alineatul (1) de la prezentul articol, autoritatea administrativă evaluează dacă utilizarea hardware-ului sau a software-ului specificat în cererea de autorizație de utilizare a hardware-ului sau a software-ului prezintă un risc pentru securitatea națională. În procesul de aprobare, autoritatea administrativă poate propune interzicerea utilizării hardware-ului sau a software-ului specificat în cererea de autorizație de utilizare a hardware-ului sau a software-ului sau stabilirea condițiilor de utilizare a acestora.

Condițiile de utilizare a hardware-ului sau a software-ului pot include, printre altele, o limită de timp pentru utilizare, utilizarea în anumite părți sau funcții sau cu o anumită configurație a rețelei de comunicații.

(3) Având în vedere dispozițiile alineatelor (1) și (2) de la prezentul articol, Autoritatea pentru protecția consumatorilor și reglementare tehnică decide asupra aprobării, a aprobării condiționate sau a refuzului de aprobare a cererii de autorizație de utilizare a hardware-ului sau a software-ului.

(4) În cazul în care hardware-ul sau software-ul nu prezintă un risc pentru securitatea națională, se acordă o autorizație de utilizare pe o perioadă de opt ani. În cazul în care hardware-ul sau software-ul prezintă un risc pentru securitatea națională, nu se acordă nicio autorizație de utilizare sau se acordă o autorizație condiționată de utilizare.

Articolul 87^5. Auditul

(1) O întreprindere de comunicații căreia i-au fost impuse obligații în temeiul articolului 87^3 din prezenta lege dispune efectuarea unui audit de conformitate cu privire la activitățile sale cel puțin o dată la trei ani după impunerea obligației, pentru a evalua în raportul de audit dacă întreprinderea de comunicații și-a îndeplinit obligațiile impuse pe baza aceluiași articol.

(2) Persoana care efectuează auditul trebuie să fie un auditor independent care deține un certificat de auditor al sistemelor informatice certificat de ISACA sau un certificat similar.

(3) Persoana care efectuează auditul depune auditul la Autoritatea pentru protecția consumatorilor și reglementare tehnică.

(4) Costurile aferente efectuării auditului sunt acoperite de întreprinderea de comunicații.

(5) Conținutul obligației de audit specificate la alineatul (1) de la prezentul articol, precum și timpul și procedura de depunere a auditului sunt stabilite printr-un regulament al Guvernului Republicii.”;

152) Legea se completează cu articolul 170^3 cu formularea următoare:

„**Articolul 170^3. Încălcarea obligațiilor impuse în scopul securității naționale**

(1) Încălcarea obligațiilor impuse în temeiul articolului 87^3 sau 87^5 din prezenta lege se pedepsește cu o amendă de până la 300 de unități de amendă.

(2) Aceeași faptă, dacă este săvârșită de o persoană juridică, se pedepsește cu o amendă de până la 50 000 EUR.”;

156) Legea se completează cu articolele 196^3-196^5, care au formularea următoare:

Articolul 196^5. Punerea în aplicare a articolelor 87^3 și 87^4 din prezenta lege

(1) Obligația de a solicita o autorizație de utilizare a hardware-ului sau a software-ului specificat la articolul 87^3 alineatul (6) din prezenta lege se aplică în cazul hardware-ului sau al software-ului implementat înainte de 1 februarie 2022 în cazul în care o funcție a 5G nu este de sine stătătoare (denumită în continuare „5G NSA”) sau un standard de rețea de comunicații mobile de generație nouă a fost sau ar urma să fie implementat în hardware sau software.

(2) Hardware-ul sau software-ul cu risc ridicat în cazul în care o funcție a 5G NSA sau a unui standard de rețea de comunicații mobile de generație mai nouă este utilizată sau ar urma să fie implementată și care nu are o funcție critică poate fi utilizată pe baza unei autorizații de

utilizare până la 31 decembrie 2025. Nu se eliberează o autorizație de utilizare pentru hardware-ul sau software-ul cu risc ridicat menționat în prima teză după 31 decembrie 2025. Termenul de depunere a cererilor de autorizare a utilizării hardware-ului sau a software-ului cu risc ridicat specificat în prima teză este stabilit în regulamentul specificat la articolul 87^3 alineatul (7) din prezenta lege.

(3) Hardware-ul sau software-ul care nu are o funcție de 5G NSA sau un standard de rețea de comunicații mobile de generație mai nouă sau o funcție critică poate fi utilizat până la 31 decembrie 2029 fără a solicita o autorizație de utilizare specificată la articolul 87^3 alineatul (6) din prezenta lege.

(4) În cazul în care hardware-ul sau software-ul specificat la alineatul (3) de la prezentul articol este destinat utilizării după 31 decembrie 2029, cererea de autorizație de utilizare trebuie depusă cel târziu la 1 iulie 2029. Nu se eliberează o autorizație de utilizare pentru hardware-ul sau software-ul cu risc ridicat menționat în prima teză după 31 decembrie 2029.

(5) Funcțiile critice ale hardware-ului și software-ului sunt: 1. funcția rețelei centrale în conformitate cu standardele Institutului European de Standardizare în Telecomunicații, indiferent de amplasarea funcției în rețeaua de comunicații; 2. funcția care are ca scop să permită autorităților de securitate și agențiilor de supraveghere să desfășoare activități de supraveghere sau să restricționeze dreptul la confidențialitatea mesajelor în cazurile prevăzute de lege.";

2. Regulamentul Guvernului Republicii nr. 119 din 16 decembrie 2021 „Modificări aduse Regulamentului Guvernului Republicii nr. 140 din 22 iunie 2006 «Cerințe pentru furnizarea de servicii de comunicare și cerințe tehnice pentru rețele de comunicații» și Regulamentului Guvernului Republicii nr. 129 din 11 decembrie 2015 «Statutul Comitetului de securitate al Guvernului Republicii".

Emitent: GUVERNUL REPUBLICII

Tip: regulament

Tip de text: text preliminar

Intrare în vigoare: 1 februarie 2022

Referință publicație: RT I, 21.12.2021, 1

Modificări aduse Regulamentului Guvernului Republicii nr. 140 din 22 iunie 2006 „Cerințe pentru furnizarea de servicii de comunicare și cerințe tehnice pentru rețele de comunicații" și Regulamentului Guvernului Republicii nr. 129 din 11 decembrie 2015 „Statutul Comitetului de securitate al Guvernului Republicii"

Adoptat la 16 decembrie 2021, nr. 119

Regulamentul este stabilit pe baza articolului 87 alineatul (2), a articolului 87^3 alineatele (5) și

(7) și a articolului 87^5 alineatul (5) din Legea privind comunicațiile electronice și a articolului 4 alineatul (2) din Legea privind apărarea națională.

Articolul 1. Modificarea Regulamentului Guvernului Republicii nr. 140 din 22 iunie 2006 „Cerințe pentru furnizarea de servicii de comunicare și cerințe tehnice pentru rețele de comunicații”

Următoarele modificări sunt aduse Regulamentului Guvernului Republicii nr. 140 din 22 iunie 2006 „Cerințe pentru furnizarea de servicii de comunicare și cerințe tehnice pentru rețele de comunicații”

1) La articolul 2 alineatul (1), articolul 3 alineatul (4a) clauza 1 și la articolul 6 alineatul (1a) din preambulul regulamentului, cuvintele „Legea privind comunicațiile electronice” se înlocuiesc cu cuvintele „Legea privind comunicațiile electronice”;

2) preambulul regulamentului se completează după cuvintele „alineatul (2)” cu cuvintele „, articolul 87^3 alineatele (5) și (7) și articolul 87^5 alineatul (5)”;

3) Alineatul (1) se modifică după cum urmează:

„Prezentul regulament stabilește:

1) cerințele pentru furnizarea de servicii publice de comunicații electronice (denumite în continuare „servicii de comunicații”) care decurg din scopurile specificate la articolul 87 alineatul (2) clauzele 1, 3 și 4 din Legea privind comunicațiile electronice;

2) cerințele tehnice și naționale de securitate pentru o rețea publică de comunicații electronice (denumită în continuare „rețea de comunicații”);

3) obligația de notificare a hardware-ului și software-ului utilizat în rețeaua de comunicații, conținutul și procedura de solicitare a unei autorizații de utilizare, precum și conținutul și procedura unei obligații de audit.”;

4) regulamentul se completează cu capitolul 2^1, care are formularea următoare:

„Capitolul 21.

CERINȚE PRIVIND SERVICIILE DE COMUNICAȚII ȘI REȚELELE DE COMUNICAȚII PENTRU ASIGURAREA SECURITĂȚII NAȚIONALE

Partea 1

Dispoziții generale

Articolul 3^1 Domeniul de aplicare al cerințelor

(1) Cerințele stabilite în prezentul capitol se aplică unei întreprinderi de comunicații care este furnizor al unui serviciu vital specificat la articolul 87 alineatul (4) din Legea privind comunicațiile electronice sau care aplică standardele 5G care nu sunt de sine stătătoare (denumite în continuare „5G NSA”) sau standardele de rețea de comunicații mobile de generație superioară ale Institutului European pentru Standarde de Telecomunicații atunci când furnizează servicii de comunicații.

(2) Cerințele stabilite în prezentul capitol nu se aplică următoarelor echipamente:

1) infrastructurii fizice a rețelei de comunicații în sensul articolului 61^2 alineatul (1) din Codul

construcţiilor;

2) elementelor de reţea care nu sunt capabile să proceseze semnale sau care nu au nevoie de energie pentru a funcţiona;

3) unităţilor de alimentare cu energie electrică;

4) unităţilor de climatizare;

5) echipamentelor terminale deţinute sau deţinute de utilizatorul final.

Partea 2

Obligaţia de notificare

Articolul 3^2 Notificarea hardware-ului şi software-ului utilizat la reţele de comunicaţii

(1) Până la data de 1 martie a fiecărui an calendaristic, o întreprindere de comunicaţii notifică Autoritatea pentru protecţia consumatorilor şi reglementare tehnică cu privire la hardware-ul şi software-ul utilizat în reţelele sale de comunicaţii începând cu data de 1 ianuarie a anului respectiv.

(2) În notificarea menţionată la alineatul (1), întreprinderea de comunicaţii trebuie să furnizeze următoarele informaţii privind hardware-ul şi software-ul utilizat în reţeaua de comunicaţii:

1. denumirea şi numărul versiunii;

2. cantitatea;

3. numele producătorului;

4. numele proprietarului;

5. numele părţilor din contractul privind dreptul de utilizare şi perioada de valabilitate a drepturilor de utilizare, dacă proprietarul hardware-ului şi al software-ului nu este întreprinderea de comunicaţii;

6. funcţia în cadrul reţelei de comunicaţii;

7. zona fizică de utilizare, care poate fi indicată ca stat, unitate administrativă, aşezare, obiect de tip adresă sau altă precizie regională;

8. existenţa sau absenţa unei autorizaţii de utilizare a hardware-ului sau a software-ului;

9. în cazul hardware-ului sau al software-ului utilizat într-o reţea mobilă, generaţia standardului de reţea mobilă cu care funcţionează hardware-ul sau software-ul;

10) o listă a persoanelor juridice care, pe lângă întreprinderea de comunicaţii, au acces administrativ hardware sau software, şi condiţiile de acces pentru fiecare persoană juridică;

11) furnizorii de servicii de întreţinere şi asistenţă pentru hardware şi software utilizate în reţeaua de comunicaţii, în mod individual de către persoane juridice, dacă acestea sunt diferite de persoanele menţionate la clauzele 4 şi 5;

12) specificarea părţilor din notificare care ar trebui să facă obiectul restricţiilor de acces în conformitate cu Legea privind informaţiile publice.

(3) Autoritatea pentru protecția consumatorilor și reglementare tehnică transmite spre informare notificarea menționată la alineatul (1) autorităților de securitate și Autorității Sistemului Informatic de Stat.

Partea 3

Obligația unei autorizații de utilizare

Articolul 3^3 Autorizația de utilizare a hardware-ului sau a software-ului și procedura de aplicare

(1) O întreprindere de comunicații trebuie să depună o cerere de autorizație de utilizare a hardware-ului sau a software-ului Autorității pentru protecția consumatorilor și reglementare tehnică înainte de utilizarea intenționată a hardware-ului sau a software-ului.

(2) O întreprindere de comunicații depune o cerere de autorizație de utilizare în termen de 10 zile lucrătoare de la implementarea hardware-ului sau a software-ului în cazul în care implementarea imediată a hardware-ului sau a software-ului este necesară pentru eliminarea sau prevenirea imediată a unui incident cibernetic în sensul Legii privind securitatea cibernetică.

(3) Într-o cerere de autorizație de utilizare, întreprinderea de comunicații prezintă informațiile menționate la articolul 3^2 alineatul (2) clauzele 1, 3-7 și 9-11 și precizează părțile din cererea de autorizație de utilizare de hardware sau software care ar trebui să facă obiectul unor restricții de acces în conformitate cu Legea privind informațiile publice.

(4) O întreprindere de comunicații poate înlocui hardware-ul și poate introduce actualizări de software fără a solicita autorizația de utilizare a hardware-ului sau a software-ului, caz în care numele sau numărul de versiune al hardware-ului sau al software-ului aprobat în autorizație se modifică, cu condiția ca celelalte informații aprobate în autorizație să rămână neschimbate.

Articolul 3^4 Prelucrarea și aprobarea cererii de autorizare pentru utilizarea de hardware sau software

(1) În termen de cinci zile lucrătoare de la primire, Autoritatea pentru protecția consumatorilor și reglementare tehnică transmite o cerere de autorizare de utilizare autorităților de securitate și Autorității Sistemului Informatic de Stat, în vederea emiterii unui aviz.

(2) În cazul în care o autoritate de securitate sau autoritatea sistemului informatic de stat constată că hardware-ul sau software-ul unei rețele de comunicații specificat într-o cerere de autorizare poate pune în pericol securitatea națională, aceasta prezintă un aviz motivat cu privire la cererea de autorizare în termen de 20 de zile lucrătoare, împreună cu o propunere de interzicere a utilizării hardware-ului sau software-ului sau de impunere a unor condiții privind utilizarea acestuia.

(3) În cazul în care autoritatea de securitate sau autoritatea sistemului informatic de stat constată într-un aviz că hardware-ul sau software-ul specificat în cerere poate pune în pericol securitatea națională, Autoritatea de protecție a consumatorilor și de reglementare tehnică oferă întreprinderii de comunicații posibilitatea de a prezenta, în termen de 20 de zile lucrătoare, un aviz privind modul în care refuzul cererii sau impunerea de condiții afectează întreprinderea de comunicații și furnizarea de servicii de comunicații, făcând, de asemenea, o propunere privind condițiile.

(4) După expirarea termenului de emitere a avizului specificat la alineatul (3), Autoritatea pentru protecția consumatorilor și reglementare tehnică trebuie să depună cererea întreprinderii de comunicații împreună cu avizele specificate la alineatele (2) și (3) la Consiliul de securitate cibernetică al Comitetului de securitate al Guvernului Republicii (denumit în continuare „Consiliul de securitate cibernetică”).

(5) În momentul aprobării, Consiliul de securitate cibernetică evaluează dacă hardware-ul sau software-ul rețelei de comunicații specificat în cererea de autorizație de utilizare este hardware sau software cu risc ridicat sau dacă utilizarea acestuia poate pune în pericol securitatea națională din cauza caracteristicilor tehnice sau a setărilor. În cazul în care hardware-ul sau software-ul poate reprezenta o amenințare la adresa securității naționale, Consiliul de securitate cibernetică evaluează condițiile în care hardware-ul sau software-ul poate fi utilizat și ia în considerare impactul refuzului sau al impunerii de condiții pentru o autorizație de utilizare a hardware-ului sau a software-ului asupra întreprinderii de comunicații, asupra continuității serviciului de comunicații și a rețelelor de comunicații, asupra pieței de comunicații și asupra concurenței și evaluează durata autorizației de utilizare.

(6) Consiliul de securitate cibernetică aprobă cererea sau refuză în mod rezonabil să o aprobe în termen de 30 de zile lucrătoare de la primirea materialelor specificate la alineatul (4). Dacă este necesar, Consiliul de securitate cibernetică poate prelungi termenul de aprobare cu până la 15 zile lucrătoare, notificând acest lucru Autorității pentru protecția consumatorilor și reglementare tehnică.

Articolul 3^5 Specificarea termenului autorizației de utilizare

La înlocuirea hardware-ului sau la actualizarea software-ului în cazul specificat la articolul 3^3 alineatul (4), durata autorizației acordate anterior pentru hardware-ul înlocuit sau software-ul actualizat continuă pentru noul hardware sau software.

Articolul 3^6 Termenul pentru procedura de autorizare

(1) Autoritatea pentru protecția consumatorilor și reglementare tehnică decide cu privire la acceptarea unei cereri de utilizare a unei întreprinderi de comunicații și la emiterea unei autorizații de utilizare în termen de 30 de zile lucrătoare de la primirea acesteia, cu excepția cazului în care este necesară procedura prevăzută la articolul 3^4 alineatele (3)-(6).

(2) În cazul în care articolul 3^4 alineatele (3)-(6) se aplică cererii, Autoritatea pentru protecția consumatorilor și reglementare tehnică decide cu privire la acceptarea sau respingerea unei cereri de autorizare de utilizare și la eliberarea unei autorizații de utilizare în termen de 105 zile lucrătoare de la primirea acesteia.

Partea 4

Obligația de audit

Articolul 3^7 Conținutul și organizarea obligației de audit

(1) Auditul de conformitate care urmează să fie comandat de o întreprindere de comunicații verifică dacă întreprinderea de comunicații a respectat obligațiile impuse în temeiul articolului 87^3 din Legea privind comunicațiile electronice și specificate în prezentul regulament.

(2) În ceea ce privește obligația de notificare a hardware-ului și software-ului, auditorul verifică dacă întreprinderea de comunicații:

1) și-a îndeplinit obligația de notificare până la termenul-limită;

2) conținutul notificării transmise corespunde cerințelor de la articolul 3^2 alineatul (2) și reflectă pe deplin hardware-ul și software-ul utilizate de întreprinderea de comunicații la momentul notificării.

(3) În ceea ce privește obligația de autorizare pentru utilizarea hardware-ului sau a software-ului, auditorul verifică dacă întreprinderea de comunicații:

1) a respectat obligația de autorizare în termenul stabilit și pentru fiecare hardware sau produs software care face obiectul obligației de autorizare;

2) a depus o cerere de autorizare pentru utilizarea hardware-ului sau a software-ului cu conținut conform cerințelor prevăzute la articolul 3^3 alineatul (3);

3) s-a bazat în mod rezonabil pe cerințele de la articolul 3^3 alineatul (2) atunci când se elimină sau se previne în mod direct un incident cibernetic;

4) a omis în mod justificat o cerere de autorizație de utilizare a hardware-ului sau a software-ului în situațiile menționate la articolul 3^3 alineatul (4).

(4) Auditorul transmite constatările auditurilor menționate la alineatele (2) și (3) Autorității pentru protecția consumatorilor și reglementare tehnică în termen de 30 de zile de la efectuarea auditului.”;

5) Regulamentul se completează cu articolele 8^1 și 8^2 care au formularea următoare:

„**Articolul 8^1. Punerea în aplicare a obligației de a depune cerere pentru o licență**

(1) O cerere de autorizație de utilizare a hardware-ului sau a software-ului care a fost dat în exploatare înainte de 1 februarie 2022 sau în perioada 1 februarie-31 mai 2022 și care include o funcție a 5G NSA sau a standardului rețelei mobile de generație superioară se depune până la 1 iunie 2022.

(2) Termenele specificate la articolul 3^4 și la articolul 3^6 alineatul (2) nu se aplică prelucrării cererii menționate la alineatul (1). Autoritatea pentru protecția consumatorilor și reglementare tehnică soluționează cererile de autorizație de utilizare a hardware-ului sau a software-ului depuse pe baza alineatului (1) până la 31 decembrie 2022.

Articolul 8^2. Punerea în aplicare a obligației de notificare a echipamentelor hardware și software utilizate în rețeaua de comunicații

Obligația de notificare menționată la articolul 3^2 alineatul (1) se îndeplinește pentru prima dată până la 1 martie 2023.”.

Articolul 2. Modificarea Regulamentului Guvernului Republicii nr. 129 din 11 decembrie 2015 „Statutul Comitetului de securitate al Guvernului Republicii”

Regulamentul Guvernului Republicii nr. 129 din 11 decembrie 2015 „Statutul Comitetului de securitate al Guvernului Republicii” se modifică după cum urmează:

1) la articolul 2 alineatul (1) din regulament, cuvintele „ministrul comerțului exterior și al tehnologiei informației” se înlocuiesc cu cuvintele „ministrul întreprinderilor și al tehnologiei informației”;

2) Regulamentul se completează cu articolul 7^1 cu formularea următoare:

Articolul 7^1. Consiliul de securitate cibernetică

(1) Consiliul de securitate cibernetică funcţionează în cadrul comisiei.

(2) Consiliul de securitate cibernetică trebuie:

1) să ofere orientări pentru dezvoltarea politicii de securitate cibernetică;

2) să adopte poziţii cu privire la planurile privind domeniul securităţii cibernetice;

3) să asigure conformitatea utilizării hardware-ului şi software-ului specificat în cererea întreprinderii de comunicaţii cu interesele de securitate ale statului;

4) să îndeplinească alte sarcini atribuite de comitet.

(3) În cadrul îndeplinirii sarcinii specificate la alineatul (2) clauza 3, consiliul de securitate cibernetică are drepturile şi obligaţiile acordate autorităţii administrative în Legea privind procedura administrativă.

(4) Consiliul de securitate cibernetică are un preşedinte şi un manager. Activitatea Consiliului de securitate cibernetică este gestionată de manager.

(5) Consiliul de securitate cibernetică include membri din următoarele ministere şi agenţii:

1) Inspectoratul pentru Protecţia Datelor;

2) Ministerul Educaţiei şi Cercetării;

3) Ministerul Justiţiei;

4) Liga pentru Apărare;

5) Ministerul Apărării;

6) Serviciul estonian de securitate internă;

7) Forţele de apărare;

8) Ministerul Mediului;

9) Ministerul Culturii;

10) Ministerul Afacerilor Rurale;

11) Ministerul Afacerilor Economice şi Comunicaţiilor;

12) Consiliul Poliţiei şi Poliţiei de Frontieră;

13) Parchetul;

14) Ministerul Finanţelor;

15) Autoritatea de Stat a Sistemului Informatic;

16) Biroul guvernamental;

17) Ministerul de Interne:

18) Ministerul Afacerilor Sociale;

19) Autoritatea pentru protecţia consumatorilor şi reglementare tehnică;

20) Agenţia de Informaţii Externe;

21) Ministerul Afacerilor Externe.

(6) Un membru supleant al Consiliului de securitate cibernetică va avea drepturile membrului înlocuit.

(7) Dacă este necesar, implicarea altor persoane în activitatea Consiliului de securitate cibernetică este organizată de către directorul Consiliului de securitate cibernetică.

(8) Consiliul de securitate cibernetică are cvorum în cazul în care cel puţin două treimi dintre membrii consiliului cu drept de vot participă la reuniune. La îndeplinirea misiunii prevăzute la alineatul (2) clauza 3, Consiliul de securitate cibernetică dispune de cvorum dacă la şedinţă participă membri ai Consiliului de securitate cibernetică din cadrul guvernului, Ministerului Apărării, Ministerului Economiei şi Comunicaţiilor, Ministerului Afacerilor Interne şi Ministerului Afacerilor Externe.

(9) Deciziile Consiliului de securitate cibernetică se iau cu majoritatea voturilor membrilor cu drept de vot prezenţi la reuniune. Guvernul şi ministerele au drept de vot. Fiecare minister şi oficiul guvernamental au câte un vot. În caz de egalitate de voturi, preşedintele Consiliului de securitate cibernetică sau, în absenţa acestuia, managerul, are votul decisiv.

(10) În îndeplinirea misiunii prevăzute la alineatul (2) punctul 3, Biroul Guvernului, Ministerul Apărării, Ministerul Economiei şi Comunicaţiilor, Ministerul de Interne şi Ministerul Afacerilor Externe au drept de vot.

(11) Regulamentul de procedură al Consiliului de securitate cibernetică se aprobă de către comitet.

(12) Regulamentul de procedură menţionat la alineatul (11) stabileşte următoarele:

1) preşedintele şi directorul Consiliului de securitate cibernetică;

2) membrii ministerelor şi agenţiilor menţionate la alineatul (5), în virtutea funcţiei lor;

3) înlocuirea membrilor, a preşedintelui şi a directorului Consiliului de securitate cibernetică;

4) alte cerinţe organizatorice.”.

Articolul 3. Intrarea în vigoare a regulamentului

Prezentul regulament intră în vigoare la 1 februarie 2022.

Jaak Aab

Ministru al Administraţiei Publice în exercitarea atribuţiilor primului-ministru

Andres Sutt

Ministrul Întreprinderilor şi Tehnologiei Informaţiei

Taimar Peterkop

Secretar de Stat