Obsah

1. Výňatky ze zákona, kterým se mění zákon o elektronických komunikacích, stavební zákon a zákon o státních poplatcích.

§ 1 Změna zákona o elektronických komunikacích

V zákoně o elektronických komunikacích jsou provedeny tyto změny:

111) § 87 odst. 2^1 a 2^2 se zrušují;

118) zákon se doplňuje o § 87^3 až 87^5 v tomto znění:

„**§ 87^3. Požadavky na komunikační sítě a služby k zajištění národní bezpečnosti**

(1) Hardware a software používaný při poskytování komunikačních služeb v komunikační síti nesmí představovat riziko pro národní bezpečnost.

(2) Hardware a software používaný při poskytování komunikačních služeb v komunikační síti může představovat riziko pro národní bezpečnost v důsledku:
1) vysokého rizika pocházejícího od jeho výrobce nebo poskytovatele služeb údržby nebo podpory (dále *vysoce rizikový hardware nebo software*);
2) rizika vyplývajícího z technických vlastností nebo konfigurace hardwaru nebo softwaru.

3)) Při posuzování vysoce rizikového hardwaru nebo softwaru se mimo jiné zohlední informace o tom, zda:
1) výrobce nebo poskytovatel údržby nebo podpůrných služeb má sídlo nebo ústředí v zemi (dále jen *země sídla*), který není členským státem Evropské unie, Organizace Severoatlantické smlouvy (dále jen *NATO*) nebo Organizace pro hospodářskou spolupráci a rozvoj (dále *OECD*);
2) nejsou dodržovány zásady demokratického právního státu nebo nejsou dodržována lidská práva v zemi sídla výrobce nebo poskytovatele služeb údržby nebo podpory;
3) duševní vlastnictví, osobní údaje nebo obchodní tajemství osob z jiných zemí nejsou chráněny v zemi sídla výrobce nebo poskytovatele služeb údržby nebo podpory;
4) země bydliště výrobce nebo poskytovatele služeb údržby nebo podpory vykazuje agresivní chování v kyberprostoru;
5) členské státy Evropské unie, NATO nebo OECD připsaly kybernetické útoky zemi sídla výrobce nebo poskytovatele služeb údržby nebo podpory;
6) výrobce nebo poskytovatel služeb údržby nebo podpory podléhá vládě nebo státnímu orgánu země sídla nebo jiné cizí země, která nemá nezávislou soudní kontrolu;
7) země sídla výrobce nebo poskytovatele služeb údržby nebo podpory nebo jiná cizí země může uložit povinnost jednat způsobem, který představuje riziko pro národní bezpečnost Estonska;
8) hospodářské činnosti výrobce nebo poskytovatele služeb údržby nebo podpory se nezakládají na hospodářské soutěži na základě trhu nebo k tomu nebyly vytvořeny odpovídající podmínky v zemi sídla;
9) vlastnická struktura, organizační struktura nebo řídící struktura výrobce nebo poskytovatele služeb údržby nebo podpory není transparentní;
10) financování výrobce nebo poskytovatele služeb údržby nebo podpory není transparentní;
11) produkty nebo služby výrobce nebo poskytovatele služeb údržby nebo podpory zahrnují zranitelná místa a nebyla zavedena žádná odpovídající bezpečnostní opatření k jejich odstranění;
12) výrobce nebo poskytovatel služeb údržby nebo podpory není schopen zajistit trvalé

dodávky výrobků nebo služeb, s výjimkou případu vyšší moci.

(4) S cílem zajistit národní bezpečnost je komunikační společnost povinna oznámit Úřadu pro ochranu spotřebitele a technickou regulaci hardware a software používaný v rámci její komunikační sítě.

(5) Rozsah oznamovací povinnosti uvedené v pododdílu 4 tohoto oddílu, jakož i zvláštní požadavky, termín pro splnění povinnosti a postup pro oznámení je stanoven nařízením vlády republiky.

(6) Pro zajištění národní bezpečnosti je komunikační společnost povinna požádat o oprávnění k používání hardwaru nebo softwaru komunikační sítě (dále jen *oprávnění k používání hardwaru nebo softwaru*) od Úřadu pro ochranu spotřebitele a technické regulace.

(7) Rozsah povinnosti požádat o oprávnění k používání hardwaru nebo softwaru, zvláštní požadavky, doba a postup řízení a specifikace týkající se doby platnosti oprávnění k užívání jsou stanoveny nařízením vlády republiky.

(8) Při vydávání předpisů uvedených v pododdílech 5 a 7 tohoto zákona bere vláda republiky v úvahu význam komunikační sítě, její hardwarové nebo softwarové a komunikační služby poskytované v síti, jakož i potenciální rizika, která z nich vyplývají pro národní bezpečnost.

§ 87[4]. Řízení o oprávnění k používání hardwaru nebo softwaru

(1) Po obdržení žádosti o oprávnění k používání hardwaru nebo softwaru požádá Úřad pro ochranu spotřebitele a technickou regulaci o stanoviska bezpečnostních orgánů a Úřadu pro informační systémy ohledně toho, zda hardware nebo software uvedený v žádosti komunikačního podniku o oprávnění k používání hardwaru nebo softwaru představuje riziko pro národní bezpečnost. Pokud může hardware nebo software podle obdrženého stanoviska představovat riziko pro národní bezpečnost, požádá Úřad pro ochranu spotřebitele a technickou regulaci o schválení orgánu uvedeného ve stanovách Bezpečnostního výboru Estonské republiky (dále jen *správní orgán*) před vyřešením žádosti komunikačního podniku o oprávnění k používání hardwaru nebo softwaru.

(2) V schvalovacím řízení uvedeném v pododdíle 1 tohoto oddílu správní orgán posoudí, zda použití hardwaru nebo softwaru uvedeného v žádosti o oprávnění k používání hardwaru nebo softwaru představuje riziko pro národní bezpečnost. V rámci schvalovacího procesu může správní orgán navrhnout zákaz používání hardwaru nebo softwaru uvedeného v žádosti o oprávnění k používání hardwaru nebo softwaru nebo stanovení podmínek pro jejich používání. Podmínky používání hardwaru nebo softwaru mohou mimo jiné zahrnovat lhůtu pro použití, použití v určitých částech nebo funkcích nebo s určitou konfigurací komunikační sítě.

(3) S ohledem na ustanovení pododdílů 1 a 2 tohoto oddílu rozhoduje Úřad pro ochranu spotřebitele a technickou regulaci o schválení, podmíněném schválení nebo zamítnutí schválení žádosti o oprávnění k používání hardwaru nebo softwaru.

(4) Pokud hardware nebo software nepředstavuje riziko pro národní bezpečnost, uděluje se oprávnění k používá na dobu 8 let. Pokud hardware nebo software představuje riziko pro národní bezpečnost, není uděleno oprávnění k používání ani podmíněné oprávnění k používání.

§ 87[5]. Audit

(1) Komunikačním společnostem, kterým byly uloženy povinnosti na základě § 87[3] podle

tohoto zákona nejméně každé tři roky po uložení povinnosti nařizuje audit dodržování předpisů za účelem toho, aby bylo ve zprávě o auditu posouzeno, zda komunikační společnost splnila povinnosti uložené na základě téhož oddílu.

(2) Osobou provádějící audit musí být nezávislý auditor, který je držitelem osvědčení o certifikaci auditora informačních systémů od ISACA nebo podobného osvědčení.

(3) Osoba provádějící audit předloží audit Úřadu pro ochranu spotřebitele a technickou regulaci.

(4) Náklady na provedení auditu hradí komunikační společnost.

(5) Obsah auditorské povinnosti uvedené v pododdíle 1 tohoto oddílu a lhůta a postup pro předložení auditu stanoví nařízení vlády republiky.“;

152) zákon se doplňuje o ustanovení § 170^3 v tomto znění:

„**§ 170^3. Porušení povinností uložených pro účely národní bezpečnosti**

(1) Porušení povinností uložených na základě § 87^3 nebo 87^5 podle tohoto zákona se trestá pokutou až do výše 300 pokutových jednotek.

(2) Za stejný čin, kterého se dopustila právnická osoba, lze uložit pokutu až do výše 50 000 EUR.“;

156) zákon se doplňuje o ustanovení § 196^3 až 196^5 v tomto znění:

§ 196^5. Provádění § 87^3 a 87^4 tohoto zákona

(1) Povinnost požádat o oprávnění k používání hardwaru nebo softwaru podle § 87^3 odst. 6 tohoto zákona se použije v případě hardwaru nebo softwaru zavedeného před 1. únorem 2022, pokud funkce 5G není samostatná (dále jen *5G NSA*) nebo norma pro mobilní komunikační sítě novější generace byla nebo by byla zavedena v hardwaru nebo softwaru.

(2) Vysoce rizikový hardware nebo software, u nichž se používá nebo by byla zavedena funkce NSA 5G nebo norma mobilní komunikační sítě nové generace a který nemá kritickou funkci, může být používán na základě oprávnění k používání do 31. prosince 2025. Oprávnění k používání se nevydává na vysoce rizikový hardware nebo software uvedený v první větě po 31. prosinci 2025. Lhůta pro podání žádostí o oprávnění k používání vysoce rizikového hardwaru nebo softwaru uvedená v první větě je stanovena v nařízení uvedeném v § 87^3 odst. 7 tohoto zákona.

(3) Hardware nebo software, který nemá funkci 5G NSA nebo normu mobilní komunikační sítě novější generace nebo kritickou funkci, může být používán do 31. prosince 2029 bez žádosti o oprávnění k používání uvedené v § 87^3 odst. 6 tohoto zákona.

(4) Je-li hardware nebo software uvedený v pododdílu 3 tohoto oddílu určen k použití po 31. prosinci 2029, musí být žádost o oprávnění k používání podána nejpozději dne 1. července 2029. Oprávnění k používání se nevydává pro vysoce rizikový hardware nebo software uvedený v první větě po 31. prosinci 2029.

(5) Kritické funkce hardwaru a softwaru jsou tyto: (1) funkce páteřní sítě v souladu s normami Evropského institutu pro telekomunikační normy bez ohledu na umístění funkce v komunikační síti; (2) funkce, jejímž cílem je umožnit bezpečnostním orgánům a agenturám dohledu provádět dohledové činnosti nebo omezit právo na důvěrnost zpráv v případech

předepsaných zákonem.“;

2. Nařízení vlády republiky č. 119 ze dne 16. prosince 2021 „Změny nařízení vlády republiky č. 140 ze dne 22. června 2006 „Požadavky na poskytování komunikačních služeb a technické požadavky na komunikační sítě“ a nařízení vlády republiky č. 129 ze dne 11. prosince 2015 „Stanovy bezpečnostního výboru vlády republiky“.

Vydala: VLÁDA ESTONSKÉ REPUBLIKY

Druh: nařízení

Druh textu: předběžné znění

Vstup v platnost: 1 Únor 2022

Uvádění publikace: RT I, 21.12.2021, 1

Změny nařízení vlády republiky č. 140 ze dne 22. června 2006 „Požadavky na poskytování komunikačních služeb a technické požadavky na komunikační sítě“ a nařízení vlády č. 129 ze dne 11. prosince 2015 „Stanovy bezpečnostního výboru vlády republiky“

Přijato dne 16. prosince 2021, č. 119

Nařízení je přijímáno na základě ustanovení § 87 odst. 2, § 87^3odst. 5 a 7 a § 87^5 odst. 5 zákona o elektronických komunikacích a § 4 odst. 2 zákona o obraně státu.

§ 1 Změna nařízení vlády republiky č. 140 ze dne 22. června 2006 „Požadavky na poskytování komunikačních služeb a technické požadavky na komunikační sítě“

V nařízení vlády republiky č. 140 ze dne 22. června 2006 „Požadavky na poskytování komunikačních služeb a technické požadavky na komunikační sítě“ se provádějí následující změny:

1) V § 2 odst. 1, § 3 odst. 4 ustanovení 1 a § 6 odst. 1 preambule nařízení se slova „zákon o elektronických komunikacích“ nahrazují slovy „zákon o elektronických komunikacích“;

2) v preambuli nařízení se za slova „odstavec 2“ doplňují slova § 87^3 odst. 5 a 7 a § 87^5 odst. 5“;

3) Odstavec 1 se mění takto:

„Tímto nařízením se stanoví:

1) požadavky na poskytování veřejných služeb elektronických komunikací (dále jen: *komunikační služby*) vyplývající z účelů uvedených v § 87 odst. 2 ustanovení 1, 3 a 4 zákona o elektronických komunikacích;

2) technické a národní bezpečnostní požadavky na veřejnou síť elektronických komunikací (dále jen: *komunikační síť*);

3) povinnost oznamovat hardware a software používané v komunikační síti, obsah a postup žádosti o oprávnění k používání a obsah a postup povinnosti auditu.“;

4) nařízení se doplňuje kapitolou 2^1, která zní takto:

„Kapitola 21

POŽADAVKY NA KOMUNIKAČNÍ SLUŽBY A KOMUNIKAČNÍ SÍTĚ K ZAJIŠTĚNÍ BEZPEČNOSTI STÁTU

Část 1

Všeobecná ustanovení

§ 3^1 Oblast použití požadavků

(1) Požadavky stanovené v této kapitole se vztahují na komunikační společnost, která je poskytovatelem životně důležité služby uvedené v § 87 odst. 4 zákona o elektronických komunikacích nebo používá normy tzv. „5G non-standalone“ (dále jen: *5G NSA*) – mobilní komunikační sítě páté nebo příští generace v nesamostatném režimu – Evropského ústavu pro telekomunikační normy při poskytování komunikačních služeb.

(2) Požadavky stanovené v této kapitole se nevztahují na následující zařízení:

1) fyzickou infrastrukturu nebo síťové prvky komunikační sítě ve smyslu § 61^2 odst. 1 stavebního zákona;

2) prvky sítě, které nejsou schopné zpracovávat signály nebo nevyžadují pro provoz energii;

3) napájecí jednotky;

4) klimatizační zařízení;

5) koncová zařízení vlastněná nebo držená koncovým uživatelem.

Část 2

Oznamovací povinnost

§ 3^2 Oznamování hardwaru a softwaru používaného v rámci komunikační sítě

(1) Do 1. března každého kalendářního roku oznamuje komunikační společnost Úřadu pro ochranu spotřebitele a technickou regulaci hardware a software používaný v rámci její komunikační sítě od 1. ledna uvedeného roku.

(2) V oznámení uvedeném v odstavci 1 poskytuje komunikační společnost níže uvedené informace o hardwaru a softwaru použitém v komunikační síti:

1) název a číslo verze;

2) množství;

3) jméno výrobce;

4) jméno majitele;

5) strany dohody o užívacím právu a doba platnosti, pokud vlastníkem hardwaru nebo softwaru není komunikační společnost;

6) funkce v komunikační síti;

7) fyzické místo použití, které lze uvést jako stát, správní jednotku, osadu, objekt adresy nebo jinou regionální upřesnění;

8) existence nebo neexistence ´oprávnění k používání hardwaru nebo softwaru;

9) v případě hardwaru nebo softwaru používaného v mobilní síti, generace normy mobilní sítě, v rámci které daný hardware nebo software funguje.

10) seznam právnických osob, které mají kromě komunikační společnosti administrativní přístup k hardwaru nebo softwaru a podmínky přístupu každé právnické osoby;

11) poskytovatelé služeb údržby a podpory hardwaru a softwaru používaného v komunikační síti, jednotlivě právnickými osobami, pokud se liší od osob uvedených v odstavcích 4 a 5;

12) upřesnění částí oznámení, které musí podléhat omezením přístupu podle zákona o veřejných informacích.

(3) Úřad pro ochranu spotřebitele a technickou regulaci předá oznámení podle pododstavce 1 pro informaci bezpečnostním orgánům a Úřadu pro státní informační systémy.

Část 3

Povinnost získat oprávnění k používání

§ 3^3 Oprávnění k používání hardwaru nebo softwaru a postup podávání žádostí

(1) Komunikační společnost předkládá žádost o udělení oprávnění k používání hardwaru nebo softwaru Úřadu pro ochranu spotřebitele a technickou regulaci před zamýšleným použitím hardwaru nebo softwaru.

(2) Komunikační společnost podá žádost o oprávnění k používání nejpozději 10. pracovní den po instalaci hardwaru nebo softwaru, pokud je hardware nebo software třeba instalovat okamžitě kvůli eliminaci nebo okamžité prevenci kybernetických útoků.

(3) Komunikační společnost v žádosti o oprávnění k užívání předloží informace uvedené v § 3^2 odst. 2 ustanoveních 1, 3 až 7 a 9 až 11 a vysvětlení, která část žádosti o oprávnění k používání hardwaru nebo softwaru má podléhat omezení přístupu ve smyslu zákona o veřejných informacích.

(4) Komunikační společnost může vyměnit hardware a zavést aktualizace softwaru, aniž by požádala o oprávnění k používání hardwaru nebo softwaru; v takovém případě se název nebo číslo verze hardwaru nebo softwaru schváleného ve změnách oprávnění, za předpokladu, že ostatní informace schválené v oprávnění zůstanou stejné.

§ 3^4 Zpracování a schválení žádosti o oprávnění k používání hardwaru nebo softwaru

(1) Úřad pro ochranu spotřebitele a technický regulační úřad předá žádost o oprávnění k používání do 5 pracovních dnů od jejího obdržení bezpečnostním orgánům a Úřadu pro státní informační systémy k vyjádření.

(2) Zjistí-li bezpečnostní orgán nebo Úřad pro státní informační systémy, že hardware nebo software komunikační sítě uvedené v žádosti o oprávnění může ohrozit národní bezpečnost, je povinen do 20 pracovních dnů předložit odůvodněné stanovisko k žádosti spolu s návrhem na

zákaz používání hardwaru nebo softwaru nebo na uložení podmínek pro jeho použití.

(3) Dojde-li bezpečnostní orgán nebo Úřad pro státní informační systém k názoru, že hardware nebo software uvedený v aplikaci může ohrozit národní bezpečnost, Úřad pro ochranu spotřebitele a technickou regulaci poskytne komunikační společnosti příležitost se ve lhůtě 20 pracovních dnů vyjádřit k tomu, jak odmítnutí použití nebo uložení podmínek ovlivní komunikační společnost, přičemž rovněž předloží návrh týkající se podmínek.

(4) Po uplynutí lhůty pro vydání stanoviska uvedené v odstavci 3 předloží Úřad pro ochranu spotřebitele a technickou regulaci žádost komunikační společnosti spolu se stanovisky uvedenými v odstavcích 2 a 3 Radě pro kybernetickou bezpečnost vlády republiky (dále jen: *Rada pro kybernetickou bezpečnost).*

(5) Rada pro kybernetickou bezpečnost po schválení posoudí, zda hardware nebo software komunikační sítě uvedené v žádosti o oprávnění k použití představuje vysoce rizikový hardware nebo software, nebo zda jeho použití může ohrozit národní bezpečnost kvůli technickým vlastnostem nebo nastavení. Pokud hardware nebo software může představovat hrozbu pro národní bezpečnost, Rada pro kybernetickou bezpečnost posoudí podmínky, za kterých lze hardware nebo software používat, a zváží dopad zákazu nebo zavedení podmínek uložených komunikační společnost pro oprávnění k používání hardwaru, komunikační trh a konkurenci a posoudí dobu platnosti oprávnění k používání.

(6) Rada pro kybernetickou bezpečnost žádost schválí nebo ji důvodně odmítne schválit do 30 pracovních dnů po obdržení materiálů uvedených v pododstavci 4. Je-li to nutné, může Rada pro kybernetickou bezpečnost prodloužit období oprávnění až o 15 pracovních dnů a oznámit to Úřadu pro ochranu spotřebitele a technickou regulaci.

§ 3[5] Upřesnění doby platnosti oprávnění k používání

Po výměně hardwaru nebo aktualizaci softwaru v případě uvedeném v § 3[3] odst. 4 pokračuje u nového hardwaru a softwaru doba dříve uděleného oprávnění, která byla udělena pro původní hardware nebo aktualizovaný software.“;

§ 3[6] Lhůta pro řízení k udělení oprávnění

(1) Orgán pro ochranu spotřebitele a technickou regulaci rozhodne o udělení oprávnění k žádosti o užívání komunikačního podniku a o vydání oprávnění k používání do 30 pracovních dnů od jejího obdržení, pokud není vyžadován postup stanovený v odstavcích v § 3[4] odst. 3 až 6.

(2) Je-li v souvislosti s aplikací komunikačního podniku nutné provést postup podle § 3[4] odst. 3 až 6, Úřad pro ochranu spotřebitele a technickou regulaci rozhodne o udělení nebo zamítnutí žádosti o oprávnění k použití a o vydání oprávnění k použití do 105 pracovních dnů po jejím obdržení.

Část 4

Povinnost auditu

§ 3[7] Obsah a organizace povinnosti auditu

(1) Audit souladu, který bude zadán komunikační společností, ověřuje, zda komunikační společnost splnila povinnosti uložené podle § 87[3] zákona o elektronických komunikacích a specifikovaných podle tohoto nařízení.

(2) Pokud jde o povinnost oznamovat hardware a software, auditor ověří, zda komunikační společnost:

1) splnila oznamovací povinnost ve stanovené lhůtě;

2) obsah předloženého oznámení odpovídá požadavkům § 3^2 odstavce 2 a plně odráží hardware a software používaný komunikační společností v době oznámení.

(3) Pokud jde o povinnost obdržet oprávnění k používání hardwaru nebo softwaru, auditor ověří, zda komunikační společnost:

1) splnila povinnost získat oprávnění ve stanovené lhůtě a pro každou položku hardwaru nebo softwaru, na kterou se vztahuje povinnost získat oprávnění;

2) podala žádost o oprávnění k používání hardwaru nebo softwaru s obsahem vyhovujícím požadavkům § 3^3odstavce 3;

3) přiměřeně vycházela z požadavků § 3^3 odstavce 2 při eliminaci nebo přímé prevenci kybernetického incidentu;

4) oprávněně opomenula podat žádost o oprávnění k používání hardwaru nebo softwaru v situacích uvedených v § 3^3 odst. 4.

(4) Auditor předloží zjištění auditů uvedených v pododdílech 2 a 3 Úřadu pro ochranu spotřebitele a technickou regulaci 30 dnů po provedení auditu.“;

5) nařízení se doplňuje o ustanovení § 8^1 a 8^2 v tomto znění:

„**§ 8^1. Zavedení povinnosti žádat o oprávnění k používání**

(1) Žádost o oprávnění k používání hardwaru nebo softwaru, které byly uvedeny do provozu před 1. únorem 2022 nebo v období od 1. února do 31. května 2022 a která zahrnuje funkci sítě 5G NSA nebo normy pro mobilní síť vyšší generace, se předloží do 1. června 2022.

(2) Lhůty uvedené v § 3^4 a pododdíl 2 § 3^6 se nevztahují na zpracování žádosti uvedené v pododdíle 1. Úřadu pro ochranu spotřebitele a technickou regulaci vyřídí žádosti o oprávnění k používání hardwaru nebo softwaru předložené na základě pododdílu 1 do 31. prosince 2022.

§ 8^2 Zavedení povinnosti oznamovat hardware a software používaný v komunikační síti

Oznamovací povinnost podle § 3 odst. 1^2 musí být poprvé splněna do 1. března 2023.“.

§ 2 Změna nařízení vlády č. 129 ze dne 11. prosince 2015 „Stanovy bezpečnostního výboru vlády republiky“

Nařízení vlády č. 129 ze dne 11. prosince 2015 „Stanovy bezpečnostního výboru vlády republiky“ se mění takto:

1) v odstavci 1 § 2 nařízení se slova „ministr zahraničního obchodu a informačních technologií“ nahrazují slovy „ministr pro podnikání a informační technologie“;

2) nařízení se doplňuje o ustanovení § 7^1 v tomto znění:

§ 7^1. Rada pro kybernetickou bezpečnost

(1) Při komisi pracuje rada pro kybernetickou bezpečnost.

(2) Rada pro kybernetickou bezpečnost:

1) poskytuje pokyny pro rozvoj politiky kybernetické bezpečnosti;

2) zaujímá stanoviska k plánům v oblasti kybernetické bezpečnosti;

3) zajišťuje soulad použití hardwaru a softwaru specifikovaného v žádosti komunikační společnosti s bezpečnostními zájmy státu;

4) vykonává další úkoly přidělené výborem.

(3) Při plnění úkolu uvedeného v odstavci 2 bodě 3 má rada pro kybernetickou bezpečnost práva a povinnosti udělené správnímu orgánu podle zákona o správním řízení.

(4) Rada pro kybernetickou bezpečnost má předsedu a ředitele. Činnost Rady pro kybernetickou bezpečnost je řízena ředitelem.

(5) Rada pro kybernetickou bezpečnost zahrnuje členy z těchto ministerstev a agentur:

1) Inspektorát pro ochranu údajů;

2) Ministerstvo školství a výzkumu;

3) Ministerstvo spravedlnosti;

4) Liga obrany;

5) Ministerstvo obrany;

6) Estonská služba vnitřní bezpečnosti;

7) Obranné síly;

8) Ministerstvo životního prostředí

9) Ministerstvo kultury;

10) Ministerstvo pro záležitosti venkova;

11) Ministerstvo hospodářství a komunikací;

12) Policejní a pohraniční stráž;

13) Státní zastupitelství;

14) Ministerstvo financí;

15) Úřad pro státní informační systémy;

16) Úřad vlády;

17) Ministerstvo vnitra;

18) Ministerstvo sociálních věcí;

19) Úřad pro ochranu spotřebitele a technickou regulaci;

20) Zahraniční zpravodajská služba;

21) Ministerstvo zahraničních věcí.

(6) Náhradní člen Rady pro kybernetickou bezpečnost má právo nahrazeného člena.

(7) V případě potřeby organizuje vedoucí Rady pro kybernetickou bezpečnost zapojení dalších osob do činnosti Rady pro kybernetickou bezpečnost.

(8) Rada pro kybernetickou bezpečnost je usnášeníschopná, pokud se zasedání zúčastní alespoň dvě třetiny členů rady s právem hlasování. Při plnění úkolu uvedeného v odstavci 3 odst. 2 je Rada pro kybernetickou bezpečnost usnášeníschopná, pokud se zasedání účastní členové Rady pro kybernetickou bezpečnost z Úřadu vlády, Ministerstva obrany, Ministerstva hospodářství a komunikací, Ministerstva vnitra a Ministerstva zahraničních věcí.

(9) Rozhodnutí Rady pro kybernetickou bezpečnost se přijímají většinou hlasů členů s právem hlasování přítomných na zasedání. Úřad vlády a ministerstva mají právo hlasovat. Každé ministerstvo a úřad vlády mají jeden hlas. V případě rovnosti hlasů je rozhodující hlas předsedy Rady pro kybernetickou bezpečnost nebo, v jeho nepřítomnosti, ředitele.

(10) Při plnění úkolu uvedeného v § 3 odst. 2 má Úřad vlády, Ministerstvo obrany, Ministerstvo hospodářství a komunikací, Ministerstvo vnitra a Ministerstvo zahraničních věcí právo hlasovat.

(11) Jednací řád Rady pro kybernetickou bezpečnost schvaluje výbor.

(12) Jednací řád uvedený v pododdílu 11 stanoví:

1) předseda a ředitel Rady pro kybernetickou bezpečnost;

2) členové ministerstev a agentur uvedených v pododdíle 5 na základě svého postavení;

3) nahrazení členů, předsedy a ředitele Rady pro kybernetickou bezpečnost;

4) další organizační požadavky.“.

§ 3 Nabytí účinnosti

Toto nařízení nabývá účinnosti dne 1. února 2022.

Jaak Aab

ministr veřejné správy ve funkci předsedy vlády

Andres Sutt

ministr pro podnikání a informační technologie

Taimar Peterkop

státní tajemník