

## Küberturvalisuse seaduse ja teiste seaduste muutmise seadus (küberturvalisuse 2. direktiivi ülevõtmine)

### § 1. Küberturvalisuse seaduse muutmine

Küberturvalisuse seaduses tehakse järgmised muudatused:

1) paragrahvi 1 täiendatakse lõigetega 1<sup>1</sup>–1<sup>6</sup> järgmises sõnastuses:

„(1<sup>1</sup>) Käesolevat seadust kohaldatakse Euroopa Liidus teenuseid osutavatele või tegutsevatele üksustele, kellel on majandusaasta jooksul keskmiselt 50 või rohkem töötajat ja kelle aasta bilansimaht või aastakäive ületab 10 miljonit eurot, arvestades mikro- ja väikese ettevõtja määratlusi Euroopa Komisjoni soovitusel 2003/361/EÜ mikro-, väikese ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.05.2003, lk 36–41). Üksuste määratlemisele ei kohaldata Euroopa Komisjoni soovitusel 2003/361/EÜ lisa artikli 3 lõiget 4.

(1<sup>2</sup>) Arvestades käesoleva paragrahvi lõiget 1<sup>1</sup>, kohaldatakse käesolevat seadust üksuse suhtes, kes on:

- 1) elektriettevõtja elektrituruseaduse tähenduses, kes tegeleb elektrienergia müügiga, kaasa arvatud edasimüügiga elektrienergia hulgimüüjale või lõpptarbijale;
- 2) jaotusvõrguettevõtja elektrituruseaduse tähenduses;
- 3) põhivõrguettevõtja elektrituruseaduse tähenduses;
- 4) elektriettevõtja elektrituruseaduse tähenduses, kes tegeleb elektrienergia tootmisega;
- 5) määratud elektriturukorraldaja Euroopa Parlamendi ja nõukogu määruse (EL) 2019/943, milles käsitletakse elektrienergia siseturgu (ELT L 158, 14.06.2019, lk 54–124), artikli 2 punkti 8 tähenduses;
- 6) turuosaline Euroopa Parlamendi ja nõukogu määruse (EL) 2019/943 artikli 2 punkti 25 tähenduses, kes osutab elektrituruseaduse tähenduses agregeerimis-, tarbimiskaja- või elektrienergia salvestamise teenust;
- 7) laadimispunkti käitaja elektrituruseaduse tähenduses, kes vastutab laadimispunkti haldamise ja käitamise eest, mis osutab lõppkasutajatele laadimisteenust, sealhulgas liikuvusteenuse osutaja nimel ja eest;
- 8) kaugkütteseaduse tähenduses kaugkütte pakkuja ja kaugjahutuse pakkuja;
- 9) nafta tootmise, rafineerimise ja töötlemise rajatistega ning nafta hoiustamise ja ülekandmisega tegelev operaator;
- 10) maagaasi, sealhulgas veeldatud maagaasi müügiga, sealhulgas maagaasi hulgimüüjale, lõpptarbijale ja maagaasi ostvale gaasiettevõtjale edasimüügiga tegelev gaasiettevõtja maagaasiseaduse tähenduses;
- 11) üksus, kes täidab maagaasi jaotamise ülesannet ja on vastutav jaotussüsteemi kasutamise eest, tagades selle hoolduse ja vajadusel arendamise teatud paikkonnas ning vajadusel maagaasivõrgu

ühendamise teiste maagaasivõrkudega ja tagab maagaasivõrgu pikaajalise võime rahuldada mõistlikku nõudlust maagaasi jaotamise järele;

12) üksus, kes täidab maagaasi ülekande ülesannet ja vastutab ülekandesüsteemi käitamise eest, tagades selle hoolduse ning vajadusel arendamise teatud paikkonnas ja vajadusel gaasivõrkude ühendamise teiste maagaasivõrkudega, ning tagab maagaasivõrgu pikaajalise võime rahuldada mõistlikku nõudlust maagaasi transportimise järele;

13) hoidlatevõrgu haldur maagaasiseaduse tähenduses;

14) veeldatud gaasi terminali haldur maagaasiseaduse tähenduses;

15) gaasiettevõtja maagaasiseaduse tähenduses;

16) maagaasi rafineerimise ja töötlemise rajatise haldur;

17) vesiniku tootmise, hoiustamise ja ülekandmisega tegelev operaator;

18) lennuettevõtja Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 097, 09.04.2008, lk 72–84), artikli 3 punkti 4 tähenduses, kes tegutseb kommertsvaldkonnas;

19) lennujaama haldaja lennundusseaduse tähenduses, Euroopa Parlamendi ja nõukogu direktiivi 2009/12/EÜ lennujaamatasude kohta (ELT L 70, 14.03.2009, lk 11–16) artikli 2 punktis 1 määratletud lennujaam ning lennujaamas olevaid abirajatiseid käitav üksus;

20) Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 549/2004, millega sätestatakse raamistik ühtse Euroopa taeva loomiseks (raammäärus) (ELT L 96, 31.03.2004, lk 1–9), artikli 2 punktis 1 määratletud lennujuhtimise teenust osutav lennuliikluskorraldusettevõtja;

21) raudteeinfrastruktuuriettevõtja ja raudteeveoettevõtja, sealhulgas teenindusrajatise käitaja raudteeseaduse tähenduses;

22) Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004 laevade ja sadamarajatiste turvalisuse tugevdamise kohta (ELT L 129, 29.04.2004, lk 6–91), I lisas meretranspordi puhul määratletud reisijate ja kauba vedamisega sisevetes, merel ja rannavetes tegelev ettevõtja, välja arvatud kõnealuse ettevõtja käidatud üksikud laevad;

23) sadama pidaja või sellise sadamarajatise valdaja sadamaseaduse tähenduses, sealhulgas nende Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004 artikli 2 punktis 11 määratletud sadamarajatised, ja sadamates tööde ning varustuse haldamisega tegelev üksus;

24) veeliikluse juhtimise keskus;

25) intelligentse transpordisüsteemi operaator liiklusseaduse tähenduses;

26) krediidiasutus Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013, krediidiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta ja määruse (EL) nr 648/2012 muutmise kohta (ELT L 176, 27.06.2013, lk 1–337), artikli 4 punkti 1 tähenduses;

27) kauplemiskoha korraldaja väärtpaberituru seaduse tähenduses;

- 28) keskne vastaspool Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (ELT L 201, 27.07.2012, lk 1–59), artikli 2 punkti 1 tähenduses;
- 29) üksus, kes tegeleb ravimiseaduse tähenduses ravimi, välja arvatud veterinaarravimi Euroopa Parlamendi ja nõukogu määruse (EL) 2019/6, mis käsitleb veterinaarravimeid ning millega tunnistatakse kehtetuks direktiiv 2001/82/EÜ (ELT L 4, 07.01.2019, lk 43–67), artikli 4 punkti 1 tähenduses, uurimise ja arendamisega;
- 30) Eurostati klassifikaatori NACE Revision 2 C jao jaotises 21 osutatud põhifarmaatsiatoote ja ravimipreparaadi tootmisega tegelev üksus;
- 31) üksus, kes toodab Euroopa Parlamendi ja nõukogu määruse (EL) 2022/123, mis käsitleb Euroopa Ravimiameti suuremat rolli ravimite ja meditsiiniseadmete alases kriisivalmiduses ja -ohjes, (ELT L 20, 31.01.2022, lk 1–37), artikli 22 tähenduses rahvatervise hädaolukorras kriitilise tähtsusega meditsiiniseadet (rahvatervise hädaolukorra esmatähtsate meditsiiniseadmete loetelu);
- 32) joogivee veeseaduse § 17 lõike 1 tähenduses varustaja ja jaotaja, välja arvatud jaotaja, kelle puhul joogivee jaotamine on väheoluline osa tema üldisest muude tarbekaupade ja kaupade tarnimistegevusest;
- 33) ettevõtja, kes tegeleb nõukogu direktiivi 91/271/EMÜ asulareovee puhastamise kohta (EÜT L 135, 30.05.1991, lk 40–52) artikli 2 punktides 1, 2 ja 3 määratletud asulareovee, olmereovee või tööstusreovee kogumise, ärajuhtimise või puhastamisega, välja arvatud ettevõtja, kelle puhul asulareovee, olmereovee või tööstusreovee kogumine, ärajuhtimine või puhastamine on väheoluline osa tema üldisest tegevusest;
- 34) interneti vahetuspunkti teenuse osutaja;
- 35) domeeninimesüsteemide süsteemi teenuse osutaja, välja arvatud juurnimeserveri operaator;
- 36) pilvandmetöötlusteenus osutaja;
- 37) andmekeskusteenus osutaja;
- 38) sisulevivõrguteenus osutaja;
- 39) hallatud teenuse osutaja;
- 40) hallatud turbeteenuste osutaja;
- 41) kosmosepõhise teenuse osutamist toetav maapealse taristu operaator, kes on Eesti Vabariigi või eraõigusliku isiku omandis, hallata või käitada, kuid kes ei ole elektroonilise side võrgu pakkuja;
- 42) postiteenus osutaja postiseaduse tähenduses, sealhulgas kulleriteenus osutaja;
- 43) ettevõtja, kelle põhitegevus on jäätmeseaduse tähenduses jäätmekäitlus, sealhulgas jäätmekäitluse järelevalve ja jäätmete kõrvaldamiseks mõeldud jäätmekäitluskoha järelehooldus;
- 44) ettevõtja, kes tegeleb Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 1907/2006, mis käsitleb kemikaalide registreerimist, hindamist, autoriseerimist ja piiramist (REACH) ja millega asutatakse Euroopa Kemikaalide Agentuur ning muudetakse direktiivi 1999/45/EÜ ja tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 793/93, komisjoni määrus (EÜ) nr 1488/94

ning samuti nõukogu direktiiv 76/769/EMÜ ja komisjoni direktiivid 91/155/EMÜ, 93/67/EMÜ, 93/105/EÜ ja 2000/21/EÜ (ELT L 396, 30.12.2006, lk 1–850), artikli 3 punktides 9 ja 14 osutatud ainete valmistamisega ning ainete või segude levitamise, ja ettevõtja, kes toodab ainetest või segudest kõnealuse määruse artikli 3 punktis 3 määratletud tooteid;

45) Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 178/2002, millega sätestatakse toidualaste õigusnormide üldised põhimõtted ja nõuded, asutatakse Euroopa Toiduohutusamet ja kehtestatakse toidu ohutusega seotud menetlused (EÜT L 31, 01.02.2002, lk 1–24 / eestikeelne eriväljaanne: peatükk 15, köide 006, lk 463–486), artikli 3 punktis 2 määratletud toidukäitlemisettevõtja, kes tegeleb hulгимүүgi, tööstusliku tootmise ja töötlemisega;

46) Euroopa Parlamendi ja nõukogu määruse (EL) 2017/745, milles käsitletakse meditsiiniseadmeid, millega muudetakse direktiivi 2001/83/EÜ, määrust (EÜ) nr 178/2002 ja määrust (EÜ) nr 1223/2009 ning millega tunnistatakse kehtetuks nõukogu direktiivid 90/385/EMÜ ja 93/42/EMÜ (ELT L 117, 05.05.2017, lk 1–175), artikli 2 punktis 1 määratletud meditsiiniseadet tootev üksus ning Euroopa Parlamendi ja nõukogu määruse (EL) 2017/746 (ELT L 117, 05.05.2017, lk 176–332) artikli 2 punktis 2 määratletud *in vitro* diagnostikameditsiiniseadmeid tootev üksus, välja arvatud käesoleva paragrahvi punktis 31 osutatud meditsiiniseadet tootev üksus;

47) Eurostati klassifikaatori NACE Revision 2 C jao jaotistes 26, 27, 28, 29 ja 30 osutatud majandustegevusega tegelev ettevõtja;

48) internetipõhise kauplemiskoha pakkuja;

49) veebipõhise otsingumootori pakkuja;

50) sotsiaalvõrguteenuse platvormi pakkuja;

51) teadusasutus.

(1<sup>3</sup>) Käesolevat seadust kohaldatakse üksuse suhtes olenemata tema suuruselt, kui üksus on:

1) üldkasutatava elektroonilise side võrgu pakkuja;

2) üldkasutatava elektroonilise side teenuse osutaja;

3) usaldusteenuse osutaja;

4) tippdomeeninimede registri pidaja;

5) domeeninimede registreerimise teenuseid osutav üksus;

6) domeeninimede süsteemi teenuse osutaja;

7) keskvalitsuse avaliku halduse üksus;

8) elutähtsa teenuse osutaja.

(1<sup>4</sup>) Käesolevat seadust kohaldatakse üksuse suhtes olenemata tema suuruselt, kui üksus vastab vähemalt ühele järgmisele tingimusele:

1) ta on sellise teenuse ainuosutaja, mis on kriitilise tähtsusega ühiskondliku või majandustegevuse säilitamiseks;

2) tema osutatava teenuse häirel võib olla oluline mõju avalikule turvalisusele, avalikule julgeolekule või rahva tervisele;

3) tema osutatava teenuse häire võib tuua kaasa olulise süsteemse riski, eelkõige sektorites, kus sellisel häirel võib olla piiriülene mõju;

4) ta on kriitilise tähtsusega oma erilise olulisuse tõttu riiklikul või piirkondlikul tasandil konkreetse sektori või teenuseliigi või riigi muude üksteisest sõltuvate sektorite jaoks.

(1<sup>5</sup>) Arvestades käesoleva paragrahvi lõike 1<sup>4</sup> punktides 1, 2, 3 ja 4 sätestatud, kohaldatakse käesolevat seadust üksuse suhtes olenemata tema suurusest, kui üksus on:

1) kohaliku tasandi avaliku halduse üksus;

2) riigi asutatud äriühing, kes osutab riigile kui ainuaktsionärile kinnisvarateenust;

3) riigi tegevusvaru haldaja;

4) kriitilise tähtsusega side-, mereraadioside ja operatiivraadiosidevõrgu teenuse osutaja;

5) avaliku teabe seaduse tähenduses andmekogu vastutav töötleja ja volitatud töötleja;

6) Arenguseire Keskus;

7) kohaliku omavalitsuse üksuste liit;

8) Riigimetsa Majandamise Keskus;

9) tervishoiuteenuste korraldamise seaduses sätestatud perearstiabi osutaja, kes ei ole elutähtsa teenuse osutaja;

10) seaduse alusel asutatud avalik-õiguslik juriidiline isik.

(1<sup>6</sup>) Vabariigi Valitsus võib käesoleva paragrahvi lõike 1<sup>4</sup> punktides 1, 2, 3 ja 4 kriteeriumitest lähtuvalt määrata määrusega valdkonna või sektori, milles oleva isiku suhtes kohaldatakse teenuse osutaja kohta sätestatud olenemata tema suurusest.“;

2) paragrahvi 1 täiendatakse lõikega 2<sup>1</sup> järgmises sõnastuses:

„(2<sup>1</sup>) Käesoleva paragrahvi lõikes 2 sätestatud erisust ei kohaldata, kui tegemist on usaldusteenuse osutajaga.“;

3) paragrahvi 1 lõige 3 tunnistatakse kehtetuks;

4) paragrahvi 1 lõige 4 muudetakse ja sõnastatakse järgmiselt:

„(4) Kui võrgu- ja infosüsteemi pidamise ning küberintsidendist teavitamise nõuded on reguleeritud välislepinguga, Euroopa Liidu õigusaktiga või muu seadusega, kohaldatakse käesolevat seadust välislepingust, Euroopa Liidu õigusaktist või muust seadusest tulenevate erisustega.“;

5) paragrahvi 1 täiendatakse lõikega 4<sup>1</sup> järgmises sõnastuses:

„(4<sup>1</sup>) Käesoleva paragrahvi lõikes 4 sätestatud erisuste esinemise korral võib valdkonna eest vastutav minister määrusega täpsustada käesoleva seaduse nõuete järgimise ulatust ja tingimusi.“;

6) seadust täiendatakse §-ga 1<sup>1</sup> järgmises sõnastuses:

**„§ 1<sup>1</sup>. Jurisdiktsioon ja territoriaalsus**

(1) Teenuse osutaja suhtes kohaldatakse selle riigi jurisdiktsiooni, kus on tema tegevuskoht või kus ta on asutatud.

(2) Erandina käesoleva paragrahvi lõikest 1, on:

1) üldkasutatava elektroonilise side võrgu pakkuja või üldkasutatava elektroonilise side teenuse osutaja jurisdiktsiooniks Euroopa Liidu liikmesriik, kus ta oma teenuseid osutab;

2) digitaalse teenuse osutaja jurisdiktsiooniks Euroopa Liidu liikmesriik, kus on tema peamine tegevuskoht;

3) keskvalitsuse avaliku halduse üksuse ja kohaliku tasandi avaliku halduse üksuse jurisdiktsiooniks Eesti Vabariik.

(3) Digitaalse teenuse osutaja peamise tegevuskoht selgitakse välja järgnevas järjekorras:

1) peamine tegevuskoht on Euroopa Liidu liikmesriik, kus turvameetmeid käsitlevad otsused valdavalt tehakse;

2) kui peamist tegevuskohta ei ole võimalik käesoleva lõike punkti 1 kohaselt kindlaks teha või kui selliseid otsuseid ei tehta Euroopa Liidus, käsitatakse peamise tegevuskohana Euroopa Liidu liikmesriiki, kus toimub küberturvalisuse alane tegevus;

3) kui peamist tegevuskohta ei ole võimalik käesoleva lõike punkti 2 kohaselt kindlaks teha, käsitatakse peamise tegevuskohana Euroopa Liidu liikmesriiki, mille territooriumil on digitaalse teenuse osutajal tegevuskoht Euroopa Liidus kõige suurema arvu töötajatega.

(4) Erisusena käesoleva paragrahvi lõikest 3, on digitaalse teenuse osutaja jurisdiktsiooniks digitaalse teenuse osutaja esindaja tegevuskoht või kus ta on asutatud, kui nimetatud esindaja on määratud.

(5) Kui digitaalse teenuse osutajal on kohustus määrata digitaalse teenuse osutaja esindaja, kuid ta pole seda määranud Euroopa Liidus, võib käesolevas seaduses sätestatud nõudeid rikkuva digitaalse teenuse osutaja vastu õiguslike meetmeid iga Euroopa Liidu liikmesriik, kus digitaalse teenuse osutaja enda teenuseid osutab.

(6) Digitaalse teenuse osutaja esindaja määramine ei piira õiguslike meetmete võtmist digitaalse teenuse osutaja suhtes.“;

7) paragrahvi 2 teksti täiendatakse punktidega 1<sup>1</sup>–1<sup>4</sup> järgmises sõnastuses:

„1<sup>1</sup>) üksus – füüsiline isik või juriidiline isik, kes on asutatud ja keda tunnustatakse tema tegevuskohajärgse riigisisese õiguse kohaselt, kes võib enda nimel omada õigusi ja kanda kohustusi;

1<sup>2</sup>) keskvalitsuse avaliku halduse üksus – üksuse üldnimetus, mille puhul on mõeldud üksustest Eesti Panka, Finantsinspektsiooni, kohtuasutust, riigi valimisteenistust, Riigikogu Kantseleid, Riigikontrolli, Vabariigi Presidendi Kantseleid, valitsusasutust, valitsusasutuse hallatav riigiasutust ja Õiguskantsleri Kantseleid;

1<sup>3</sup>) kohaliku tasandi avaliku halduse üksus – üksuse üldnimetus, mille puhul on mõeldud üksustest kohaliku omavalitsuse üksust, valla või linna ametiasutust, valla või linna ametiasutuse hallatavat asutust, osavald, linnaosa, osavalla või linnaosa ametiasutust, osavalla või linnaosa ametiasutuse hallatavat asutust ning kohaliku omavalitsuse üksuste ühisametit ja -asutust;

1<sup>4</sup>) küberturvalisus – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 07.06.2019, lk 15–69), artikli 2 punktis 1 määratletud küberturvalisus;“;

8) paragrahvi 2 punktis 2 asendatakse sõna „tegevusele“ sõnaga „sündmusele“;

9) paragrahvi 2 teksti täiendatakse punktidega 3<sup>1</sup>–3<sup>9</sup> järgmises sõnastuses:

„3<sup>1</sup>) ulatuslik küberintsident – küberintsident, mille põhjustatud häired on niivõrd laialdased, et üks liikmesriik ei suuda nendega toime tulla või millel on märkimisväärne mõju vähemalt kahele liikmesriigile;

3<sup>2</sup>) küberintsidendi käsitlemine – toimingud ja menetlused, mille eesmärk on küberintsidendi ennetada, tuvastada, analüüsida, ohjata või lahendada ja sellest taastuda;

3<sup>3</sup>) risk – küberintsidendist tingitud kahju või häire võimekus, mida tuleb väljendada sellise kahju või katkestuse ulatust ja kõnealuse küberintsidendi esinemise võimalikkust arvesse võtva kombineeritud näitajana;

3<sup>4</sup>) küberoht – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punktis 8 määratletud küberoht;

3<sup>5</sup>) oluline küberoht – küberoht, mille tehniliste näitajate põhjal võib eeldada, et sellel võib olla tõsine mõju teenuse osutaja süsteemile või üksuse süsteemide kasutajatele, tekitades märkimisväärset varalist või mittevaralist kahju;

3<sup>6</sup>) nõrkus – IKT-toote või -teenuse nõrkus, tundlikkus või viga, mida küberohu tekitaja võib ära kasutada;

3<sup>7</sup>) IKT-toode – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punktis 12 määratletud IKT-toode;

3<sup>8</sup>) IKT-teenus – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punktis 13 määratletud IKT-teenus;

3<sup>9</sup>) IKT-protsess – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punktis 14 määratletud IKT-protsess;“;

10) paragrahvi 2 punkt 4 tunnistatakse kehtetuks;

11) paragrahvi 2 teksti täiendatakse punktidega 4<sup>1</sup>–4<sup>7</sup> järgmises sõnastuses:

„4<sup>1</sup>) interneti vahetuspunkt – võrgustik, mis võimaldab rohkem kui kahe sõltumatu võrgu omavahelist ühendamist, eelkõige selleks, et hõlbustada internetiliikluse vahetust; see võimaldab üksnes autonoomsete süsteemide omavahelist ühendamist ega nõua kahe osaleva autonoomse süsteemi vahel toimuva internetiliikluse kulgemist mõne kolmanda autonoomse süsteemi kaudu, ei muuda sellist liiklust ega sekku sellesse mingil muul viisil;

4<sup>2</sup>) domeeninimede süsteem – hierarhiline ja hajus nimesüsteem, mis võimaldab tuvastada internetiteenuseid ja -ressursse, võimaldades lõppkasutaja seadmetel kasutada internetimarsruutimise ja ühenduvuse teenuseid, et jõuda nende teenuste ja ressursideni;

4<sup>3</sup>) domeeninimede süsteemi teenuse osutaja – üksus, kes osutab interneti lõppkasutajatele üldsusele kättesaadavat domeeninime rekursiivse teisendamise teenust, või kolmandatele isikutele kasutuseks domeeninime autoriteetse teisendamise teenust, välja arvatud juurnimeserverid;

4<sup>4</sup>) tippdomeeninimede register – üksus, kellele on delegeeritud Eesti maatumnusega seotud tippdomeen ja kes vastutab selle tippdomeeni haldamise eest, sealhulgas tippdomeeni alldomeeninimede registreerimise eest ja tippdomeeni tehnilise toimimise eest, sealhulgas nimeserverite käitamise, andmebaaside hooldamise ning nimeserverite vahel tippdomeeni tsoonifailide jaotamise eest, olenemata sellest, kas mõne neist toimingutest teeb üksus ise või ostetakse need sisse, kuid välja arvatud olukorrad, kus tippdomeeninimesid kasutab register ise ainult enda tarbeks;

4<sup>5</sup>) domeeninimede registreerimise teenuseid osutav üksus – tippdomeeninimede registri registripidaja või registripidaja nimel tegutsev esindaja, näiteks registreerimisega seotud privaatsusteenuse või proksiteenuse osutaja või edasimüüja;

4<sup>6</sup>) usaldusteenuse osutaja – Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.08.2014, lk 73–114), artikli 3 punktis 19 määratletud usaldusteenuse osutaja;

4<sup>7</sup>) kvalifitseeritud usaldusteenuse osutaja – Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 3 punktis 20 määratletud kvalifitseeritud usaldusteenuse osutaja;“;

12) paragrahvi 2 punktid 5–7 muudetakse ja sõnastatakse järgmiselt:

„5) internetipõhine kauplemiskoht – internetipõhine kauplemiskoht tarbijakaitseseaduse tähenduses;



6) veebipõhine otsingumootor – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/1150, mis käsitleb õigluse ja läbipaistvuse edendamist veebipõhiste vahendusteenuste ärikasutajate jaoks (ELT L 186, 11.07.2019, lk 57–79), artikli 2 punktis 5 määratletud veebipõhine otsingumootor;

7) pilvandmetöötlusteenus – infoühiskonna teenus, mis võimaldab jagatavate andmetöötlusressursside skaleeritava ja paindliku kogumi nõudepõhist haldamist ning ulatuslikku kaugpääsu sellele kogumile, sealhulgas juhul, kui need ressursid paiknevad hajutatult erinevates kohtades;“;

**13)** paragrahvi 2 teksti täiendatakse punktidega 7<sup>1</sup>–7<sup>5</sup> järgmises sõnastuses:

„7<sup>1</sup>) andmekeskusteenus – teenus, mis hõlmab struktuure või struktuuride rühmi, mis on ette nähtud andmete talletamiseks, töötlemiseks ja edastamiseks kasutatavate infotehnoloogia- ja võrguseadmete keskseks majutamiseks, omavahel sidumiseks ja käitamiseks, sealhulgas kõiki energiajaotuse ja keskkonnakontrolliga seotud vahendeid ja taristuid;

7<sup>2</sup>) sisulevivõrk – geograafiliselt hajutatud serverite võrk, mille eesmärk on tagada digisisu ja infoühiskonna teenuse laialdane kättesaadavus, neile juurdepääsetavus või nende kiire edastamine internetikasutajatele sisu- ja teenusepakkujate nimel;

7<sup>3</sup>) sotsiaalvõrguteenuse platvorm – platvorm, mis võimaldab lõppkasutajatel vastastikku ühendust pidada, sisu jagada, teavet otsida ja suhelda mitme seadme kaudu, eelkõige vestluste, postituste, videote ja soovitude vormis;

7<sup>4</sup>) digitaalse teenuse osutaja – üksuse üldnimetus, mille puhul on mõeldud üksustest domeeninimede süsteemi teenuse osutajat, tippdomeeninimede registrit, domeeninimede registreerimise teenuseid osutavat üksust, pilvandmetöötlusteenuse osutajat, andmekeskusteenuse osutajat, sisulevivõrkude pakkujat, hallatud teenuse osutajat, hallatud turbeteenuste osutajat, internetipõhise kauplemiskoha, veebipõhise otsingumootori või sotsiaalvõrguteenuse platvormi pakkujat;

7<sup>5</sup>) digitaalse teenuse osutaja esindaja – Euroopa Liidus asuv füüsiline või juriidiline isik, kes on määratud tegutsema väljaspool Euroopa Liitu asuva digitaalse teenuse osutaja nimel ja kelle poole võib Riigi Infosüsteemi Amet pöörduda seoses digitaalse teenuse osutaja kohustustega;“;

**14)** paragrahvi 2 teksti täiendatakse punktidega 9–13 järgmises sõnastuses:

„9) üldkasutatav elektroonilise side võrk – elektroonilise side seaduse tähenduses üldkasutatav elektroonilise side võrk;

10) elektroonilise side teenus – elektroonilise side seaduse tähenduses elektroonilise side teenus;

11) hallatud teenuse osutaja – üksus, kes osutab teenuseid, mis on seotud IKT-toodete, võrkude, taristu, rakenduste või muude süsteemide paigaldamise, haldamise, käitamise või hooldamisega toe või aktiivse haldamise kaudu kas klientide ruumides või kaugteel;

12) hallatud turbeteenuste osutaja – hallatud teenuste osutaja, kes viib ellu küberturvalisuse riskijuhtimisega seotud tegevust või pakub selleks tuge;

13) teadusasutus – üksus, kelle peamine eesmärk on viia ellu rakendusuuringuid või tootearendust eesmärgiga kasutada selliste teadusuuringute tulemusi ärilistel eesmärkidel, kuid mis ei hõlma haridusasutusi.“;

15) paragrahvi 3 lõige 1 tunnistatakse kehtetuks;

16) paragrahvi 3 täiendatakse lõigetega 1<sup>1</sup>–1<sup>4</sup> järgmises sõnastuses:

„(1<sup>1</sup>) Teenuse osutaja käesoleva seaduse tähenduses on elutähtis üksus ja oluline üksus.

(1<sup>2</sup>) Elutähtis üksus on:

- 1) kvalifitseeritud usaldusteenuse osutaja;
- 2) tippdomeeninimede registri pidaja;
- 3) domeeninimede süsteemi teenuse osutaja;
- 4) keskvalitsuse avaliku halduse üksus;
- 5) kohaliku tasandi avaliku halduse üksus;
- 6) elutähtsa teenuse osutaja;
- 7) kriitilise tähtsusega side-, mereraadioside ja operatiivraadiosidevõrgu teenuse osutaja;
- 8) riigi tegevusvaru haldaja;
- 9) üldkasutatava elektroonilise side võrgu või üldkasutatava elektroonilise side teenuse pakkuja, kellel on majandusaasta jooksul keskmiselt 50 või rohkem töötajat ja kelle aasta bilansimaht või aastakäive ületab 10 miljonit eurot, arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovitusel 2003/361/EÜ;
- 10) üksus, kellel on majandusaasta jooksul keskmiselt 250 või rohkem töötajat ja kelle aasta bilansimaht ületab 50 miljonit eurot või aastakäive ületab 43 miljonit eurot, arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovitusel 2003/361/EÜ, ning kes on osutatud vähemalt ühes käesoleva seaduse § 1 lõike 1<sup>2</sup> punktides 1–51.

(1<sup>3</sup>) Oluline üksus on:

- 1) üldkasutatava elektroonilise side võrgu või üldkasutatava elektroonilise side teenuse pakkuja, kes ei ole elutähtis üksus;
- 2) usaldusteenuse osutaja, kes ei ole elutähtis üksus;
- 3) tervishoiuteenuste korraldamise seaduses sätestatud perearstiabi osutaja, kes ei ole elutähtsa teenuse osutaja;
- 4) avaliku teabe seaduse tähenduses andmekogu vastutav töötaja ja volitatud töötaja, kes ei ole elutähtis üksus;
- 5) Arenguseire Keskus;
- 6) kohaliku omavalitsuse üksuste liit;
- 7) Riigimetsa Majandamise Keskus;

- 8) seaduse alusel asutatud avalik-õiguslik juriidiline isik;
- 9) riigi asutatud äriühing, kes osutab riigile kui ainuaktsionärile kinnisvarateenust;
- 10) üksus, kellel on majandusaasta jooksul keskmiselt rohkem kui 50 töötajat ja kelle aasta bilansimaht on vahemikus 10–43 miljonit eurot ning aastakäive on vahemikus 10–50 miljonit eurot, arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovitusel 2003/361/EÜ, ja kes on osutatud vähemalt ühes käesoleva seaduse § 1 lõike 1<sup>2</sup> punktides 1–51.
- (1<sup>4</sup>) Käesoleva seaduse § 1 lõike 1<sup>6</sup> alusel antud Vabariigi Valitsuse määruse andmisel sätestatakse samas määruhes, kas teenuse osutaja on elutähtis üksus või oluline üksus.“;

**17)** paragrahvi 3 lõige 2 tunnistatakse kehtetuks;

**18)** paragrahvi 3 lõige 3 muudetakse ja sõnastatakse järgmiselt:

„(3) Riigi Infosüsteemi Amet tuvastab iga kahe aasta tagant käesoleva seaduse kohaldamisalas olevad teenuse osutajad ja domeeninimede registreerimise teenuseid osutavad üksused, kes tegutsevad Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152), elutähtsate üksuste ja oluliste üksustena ning domeeninimede registreerimise teenuseid osutavate üksustena.“;

**19)** paragrahvi 3 täiendatakse lõigetega 3<sup>1</sup>–3<sup>4</sup> järgmises sõnastuses:

„(3<sup>1</sup>) Teenuse osutaja ja domeeninimede registreerimise teenuseid osutav üksus esitab Riigi Infosüsteemi Ametile vähemalt järgmise teabe:

- 1) nimi ja registrikood;
- 2) aadress ja ajakohased kontaktandmed, sealhulgas e-posti aadressid, interneti protokollide aadresside vahemikud ja telefoninumbrid;
- 3) asjakohasel juhul Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 lisas I või II osutatud asjakohane sektor ja allsektor;
- 4) asjakohasel juhul nende riikide loetelu, kus ta osutab Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 kohaldamisalasse kuuluvaid teenuseid.

(3<sup>2</sup>) Teenuse osutaja ja domeeninimede registreerimise teenuseid osutav üksus teatab kõigist käesoleva paragrahvi lõike 3<sup>1</sup> kohaselt esitatud teabes toimunud muudatustest viivitamata ja igal juhul kahe nädala jooksul alates muutuse kuupäevast.

(3<sup>3</sup>) Riigi Infosüsteemi Amet teatab iga kahe aasta järel:

- 1) Euroopa Komisjonile ja Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 14 nimetatud koostöörühmale (edaspidi *koostöörühm*) iga sama direktiivi lisas I või II osutatud

sektori ning allsektori kohta käesoleva paragrahvi lõikes 3 nimetatud teenuse osutajate loetelus sisalduvate teenuse osutajate arvu;

2) Euroopa Komisjonile käesoleva seaduse § 1 lõigete 1<sup>3</sup> ja 1<sup>4</sup> kohaselt kindlaks määratud teenuse osutajate arvu, Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 lisas I ja II osutatud sektori ning allsektori info, nende osutatavate teenuste liigi info koos teabega, millise käesoleva seaduse § 1 lõike 1<sup>4</sup> punktide 1–4 kohaselt need teenuse osutajad kindlaks määrati.

(3<sup>4</sup>) Teenuse osutaja ja domeeninimede registreerimise teenuseid osutav üksus võib lähtuda Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 3 lõike 4 alusel antud Euroopa Komisjoni suunistest ja vormidest, kui need on kehtestatud.“;

**20)** paragrahvi 3 lõige 4 tunnistatakse kehtetuks;

**21)** paragrahv 4 muudetakse ja sõnastatakse järgmiselt:

#### **„§ 4. Digitaalse teenuse osutaja**

(1) Digitaalse teenuse osutaja esitab Riigi Infosüsteemi Ametile vähemalt järgmise teabe:

1) nimi ja registrikood;

2) asjakohasel juhul teabe Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 lisas I või II osutatud asjakohase sektori, allsektori ja üksuse liigi kohta;

3) peamise tegevuskoha ja Euroopa Liidus asuvate muude ametlike tegevuskohtade aadress või kui tal Euroopa Liidus tegevuskohta ei ole või ta ei ole seal asutatud, tema digitaalse teenuse osutaja esindaja aadress;

4) enda ja asjakohasel juhul digitaalse teenuse osutaja esindaja ajakohased kontaktandmed, sealhulgas e-posti aadressid ja telefoninumbrid;

5) liikmesriigid, kus teenust osutatakse;

6) interneti protokollide aadresside vahemikud.

(1<sup>1</sup>) Digitaalse teenuse osutaja teatab kõigist käesoleva paragrahvi lõike 1 kohaselt esitatud teabes toimunud muudatustest viivitamata ja igal juhul hiljemalt kolme kuu jooksul alates muutuse kuupäevast.

(1<sup>2</sup>) Riigi Infosüsteemi Amet esitab käesoleva paragrahvi lõike 1 punktides 1–5 osutatud teabe põhjendamatu viivitusega Euroopa Liidu Küberturvalisuse Ametile.

(1<sup>3</sup>) Riigi Infosüsteemi Amet võib esitada Euroopa Liidu Küberturvalisuse Ametile taotluse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 27 lõikes 1 nimetatud registreile juurdepääsu saamiseks.

(1<sup>4</sup>) Digitaalse teenuse osutaja võib lähtuda Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 3 lõike 4 alusel antud Euroopa Komisjoni suunistest ja vormidest, kui need on kehtestatud.

(2) Eestis teenust osutav, kuid väljaspool Euroopa Liitu asutatud digitaalse teenuse osutaja peab määrama digitaalse teenuse osutaja esindaja Eestis või mõnes teises Euroopa Liidu liikmesriigis, kus ta teenust osutab või kus ta on asutatud, ja tegema püsivalt avalikult kättesaadavaks nimetatud esindaja kontaktandmed.“;

**22)** paragrahvi 5 muudetakse ja sõnastatakse järgmiselt:

**„§ 5. Pädevad asutused ja ülesanded**

(1) Vabariigi Valitsus võtab vastu Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 7 nimetatud küberturvalisuse strateegia, mis võib olla koostatud muu õigusakti alusel koostatava dokumendi osa. Justiits- ja Digiministeerium koordineerib küberturvalisuse strateegia koostamist, sealhulgas täidab Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 7 lõigetes 3 ja 4 sätestatud nõudeid.

(2) Justiits- ja Digiministeerium ning Riigi Infosüsteemi Amet osalevad koostöörühma tegevustes vastavalt koostöörühma ülesannetele.

(3) Riigi Infosüsteemi Amet täidab Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555:

1) artikli 8 lõikes 1 nimetatud pädeva asutuse ja lõikes 3 nimetatud ühtse kontaktpunkti ülesandeid;

2) artikli 9 lõikes 1 nimetatud ulatuslike küberintsidentide ja kriiside ohjamise eest vastutava pädeva asutuse ülesandeid;

3) artikli 10 lõikes 1 nimetatud küberturbe intsidentide lahendamise üksuse ülesandeid;

4) artikli 12 lõikes 1 nimetatud nõrkuste koordineeritud avalikustamise koordinaatori ülesandeid;

5) artiklis 15 nimetatud riiklike küberturbe intsidentide lahendamise üksuste võrgustikus osalemise ülesandeid;

6) artiklis 16 nimetatud Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikus osalemise ülesandeid.

(4) Küberturbe intsidentide lahendamise üksus peab:

1) hõlmama oma tegevustesse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 lisades I ja II osutatud sektoreid, allsektoreid või üksuste liike ning vastutama küberintsidentide käsitlemise eest kindla menetluse kohaselt;

2) tagama oma sidekanalite laialdase kättesaadavuse, vältides nõrku lülisid, ja kasutama mitmesuguseid vahendeid, mis võimaldavad tal teistega ning teistel temaga igal ajal ühendust võtta;

3) määrama kindlaks sidekanalid ja tegema need oma sihtrühmadele ning koostööpartneritele teatavaks;

4) tagama, et tema ametiruumid ja tööd toetavad süsteemid asuvad turvalises kohas;

5) tagama, et tal on olemas päringute haldamiseks ja suunamiseks sobiv süsteem, mis võimaldab ka tööde tõhusat üle andmist;

- 6) tagama oma tegevuse konfidentsiaalsuse ja usaldusväärsuse;
  - 7) omama piisavat arvu töötajaid ja ametnikke, et tagada enda teenuste pidev kättesaadavus;
  - 8) tagama oma töötajatele ja ametnikele asjakohase väljaõppe;
  - 9) oma teenuste toimepidevuse tagamiseks omama varusüsteeme ja -tööruume.
- (5) Küberturbe intsidentide lahendamise üksusel on järgmised ülesanded ja volitused:
- 1) osaleb käesoleva seaduse §-s 17<sup>5</sup> sätestatud vastastikusel hindamises;
  - 2) teeb koostööd teiste küberturbe intsidentide lahendamise üksustega;
  - 3) võib teha kolmandate riikide riiklike küberturbe intsidentide lahendamise üksustega või samaväärsete kolmandate riikide asutustega koostööd, eelkõige küberturvalisuse alase abi andmiseks;
  - 4) teeb koostööd teenuse osutajate sektoripõhiste või -vaheliste kogukondadega, sealhulgas vajadusel vahetades nendega teavet arvestades käesoleva seaduse §-s 17<sup>5</sup> sätestatud nõudeid.
  - 5) võib osaleda rahvusvahelistes koostöövõrgustikes;
  - 6) korraldab küberohtude, nõrkuste ja intsidentide seiret ning analüüsi riiklikul tasandil;
  - 7) taotluse korral osutab abi asjaomastele teenuse osutajatele nende süsteemide reaalajas või reaalajalähedase seirega;
  - 8) tagab küberohtude, nõrkuste ja küberintsidentide kohta varajaste hoiatuste, hoiatuste ja teadete edastamise ning teabe levitamise asjaomastele teenuse osutajatele, pädevatele asutustele ja muudele asjaomastele sidusrühmadele, võimaluse korral reaalajalähedaselt;
  - 9) lahendab küberintsidente ja asjakohasel juhul abistab asjaomaseid teenuse osutajaid;
  - 10) kogub ja analüüsib kohtuekspertiisiandmeid, analüüsib järjepidevalt riske ja küberintsidente, ning tagab küberturvalisuse alast olukorrateadlikkust;
  - 11) potentsiaalselt olulise mõjuga nõrkuste kindlaks tegemiseks ennetavalt kontrollib teenuse osutaja taotlusel teenuse osutaja süsteemi;
  - 12) osaleb riiklike küberturbe intsidentide lahendamise üksuste võrgustikus ja osutab teisele võrgustiku liikme taotluse korral samale liikmele oma võimekusele ja pädevusele vastavat vastastikust abi;
  - 13) tegutseb käesoleva paragrahvi lõike 3 punktis 4 sätestatud ülesannetes;
  - 14) panustab teenuse osutajatega ja asjaomaste sidusrühmadega teabe vahetamiseks kasutatavate turvaliste teabejagamisvahendite kasutuselevõtmisse;
  - 15) võib teenuse osutaja üldkasutatavat süsteemi ennetavalt väliselt kontrollida, kui see toimub nõrkade või ebaturvaliselt configureeritud süsteemi tuvastamiseks ja asjaomase teenuse osutaja teavitamiseks, ning sellisel kontrollimisel ei tohi olla negatiivset mõju teenuse osutaja osutatava teenuse toimimisele;
  - 16) loob koostöösuhteid erasektori asjaomaste sidusrühmadega.

(6) Küberturbe intsidentide lahendamise üksus võib käesoleva paragrahvi lõike 5 punktides 6–14 sätestatud ülesandeid riski- või ohuprognooosi põhise lähenemisviisi alusel teatavaid ülesandeid prioriseerida.

(7) Käesoleva paragrahvi lõike 4 punktis 16 nimetatud koostöö hõlbustamiseks toetab küberturbe intsidentide lahendamise üksus ühtsete või standardsete tavade, liigitamissüsteemide ja taksonoomiate kasutuselevõttu seoses küberintsidentide käsitlemise menetlustega, kriisiohjega ning nõrkuste koordineeritud avalikustamisega.

(8) Küberturbe intsidentide lahendamise üksus käesoleva paragrahvi lõike 3 punktis 4 oleva ülesande täitmisel:

1) tegutseb usaldusväärse vahendajana, hõlbustades vajadusel suhtlust nõrkusest teavitava füüsilise või juriidilise isiku ja potentsiaalse nõrkusega IKT-toodete tootja või IKT-teenuste osutaja vahel, tegutsedes ükskõik kumma poole taotlusel;

2) teeb kindlaks teavitatud potentsiaalse nõrkuse või nõrkusega seotud teenuse osutaja ja võtab temaga ühendust;

3) abistab potentsiaalsest nõrkusest ja nõrkusest teavitavat füüsilist või juriidilist isikut;

4) peab läbirääkimisi nõrkusest avalikkuse teavitamise tähtaja üle;

5) haldab mitut teenuse osutajat mõjutavaid nõrkusi.

6) tagab, et teatatud nõrkusega seoses võetakse hoolikaid järelmeetmeid;

7) tagab potentsiaalsest nõrkusest või nõrkusest teatava füüsilise või juriidilise isiku anonüümsuse;

8) teeb teise liikmesriigi poolt Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 15 nimetatud riiklike küberturbe intsidentide lahendamise üksuste võrgustikus nõrkuste koordineeritud avalikustamise koordinaatori ülesandeid täitva küberturbe intsidentide lahendamise üksusega koostööd, kui teates esitatud nõrkus võib oluliselt mõjutada teenuse osutajaid rohkem kui ühes Euroopa Liidu liikmesriigis.

(9) Julgeolekuasutus täidab Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 8 lõikes 1 nimetatud pädeva asutuse ülesandeid käesoleva seaduse §-s 14 sätestatud ulatuses.“;

**23)** seadust täiendatakse §-ga 5<sup>2</sup> järgmises sõnastuses:

**„§ 5<sup>2</sup>. Piiriüleste elektrivoogude küberturvalisuse valdkonna pädev asutus**

(1) Riigi Infosüsteemi Amet täidab Euroopa Komisjoni delegeeritud määruse (EL) 2024/1366, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2019/943 ning kehtestatakse võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta (ELT L, 24.05.2024, lk 1–44), artikli 4 lõikes 1 nimetatud pädeva asutuse ülesandeid.

(2) Valdkonna eest vastutav minister võib volitada Riigi Infosüsteemi Ametit käesoleva paragrahvi lõikes 1 nimetatud ülesande täitmise edasi volitada, arvestades Euroopa Komisjoni delegeeritud määruse (EL) 2024/1366 artikli 4 lõikes 3 ja halduskoostöö seaduses sätestatud nõudeid.

(3) Vabariigi Valitsus võib Euroopa Komisjoni delegeeritud määruse (EL) 2024/1366 artikli 39 lõikes 4, artikli 40 lõikes 5 ning artikli 41 lõikes 4 viidatud ülesande täitmise edasi volitada Euroopa Parlamendi ja nõukogu määruse (EL) 2019/943, milles käsitletakse elektrienergia siseturgu (ELT L 158, 14.06.2019, lk 54–124), artikli 35 kohaselt asutatud piirkondlikule koordineerimiskeskusele, arvestades halduskoostöö seaduses sätestatud nõudeid.“;

**24)** seadust täiendatakse §-ga 6<sup>1</sup> järgmises sõnastuses:

**„§ 6<sup>1</sup>. Teenuse osutaja juhtorgani kohustused**

(1) Teenuse osutaja juhtorgan kiidab heaks turvameetmed, jälgib nende rakendamist ja vastutab nende täitmise eest.

(2) Teenuse osutaja juhtorgani liige peab läbima korrapäraselt erikoolitusi, mille õpiväljunditeks on piisavate teadmiste ja oskuste omandamine, et mõista ja hinnata küberturvalisuse riske, nendest tulenevat mõju teenuse osutaja osutatavatele teenustele ning viise riskide käsitlemiseks.

(3) Teenuse osutaja juhtorgan tagab, et teenuse osutaja töötajad ja ametnikud saavad korrapäraselt sarnaseid koolitusi teemadel, mis on nimetatud käesoleva paragrahvi lõikes 2.“;

**25)** paragrahvi 7 lõige 1 muudetakse ja sõnastatakse järgmiselt:

„(1) Teenuse osutaja rakendab alaliselt asjakohased ja proportsionaalsed tehnilised, tegevuslikud ning korralduslikud turvameetmed, et:

1) hallata riske, mis ohustavad teenuse osutaja tegevuses või teenuse osutamisel kasutatava süsteemi turvalisust;

2) ennetada või minimeerida küberintsidendi mõju teenuse osutaja osutatava teenuse saajale ja muule teenusele; ning;

3) ennetada, avastada ja lahendada küberintsidenti.“;

**26)** paragrahvi 7 lõike 2 punktid 1–3 muudetakse ja sõnastatakse järgmiselt:

„(2) Teenuse osutaja on turvameetmete rakendamisel kohustatud:

1) koostama ja kehtestama infoturvariskide kaalutlemise meetodika ja protseduurid;

2) koostama ja kehtestama infoturbe eesmärgid ja infoturvapoliitika;

3) koostama ja kehtestama küberintsidentide avastamise ja halduse protseduurid;

4) võtma kasutusele abinõud küberintsidendi mõju ja leviku vähendamiseks, sealhulgas vajaduse korral piirama süsteemi kasutamist või juurdepääsu süsteemile;

5) tagama süsteemi talitluspidevuse, sh süsteemi varundus- ja taasteprotseduuride toimimise;

6) tagama süsteemi tarneahela turvalisuse, sh teenuse osutaja ja tema koostööpartnerite vaheliste lepetes turvameetmetega seotud aspektide regulaarse ülevaatus ja ajakohastamise;

7) tagama süsteemi hankimise, arendamise ja hooldamise turvalisuse, sh nõrkuste käsitlemise ning avalikustamise;



- 8) kehtestama protsessi turvameetmete regulaarseks läbivaatuseks, turvameetmete tõhususe hindamiseks ja infoturbe parendamiseks;
- 9) koolitama regulaarselt kõiki teenuse osutaja ametnikke ja töötajaid küberhügieeni ning küberturvalisuse tagamise osas;
- 10) kasutama asjakohasel juhul krüptograafilisi meetmeid;
- 11) koostama ja kehtestama pääsuhalduse poliitika ja seotud protseduurijuhendid;
- 12) koostama ja kehtestama varade halduse põhimõtted ja seotud protseduurijuhendid;
- 13) asjakohasel juhul kasutama mitmik- või pidevautentimise meetodit või lahendust, turvalise hääl-, video- ja tekstiside sidelahendust, ning kriisiolukorras kasutatavat turvalist sidelahendust;
- 14) viima läbi süsteemi riskide kaalutlemist, mille käigus koostatakse süsteemi turvalisust ja selle toimepidevust mõjutavate ning küberintsidendi tekkimist põhjustavate riskide loetelu, määratakse riskide realiseerumise tagajärgede raskusaste ning kirjeldatakse riskikäsitlusmeetmed.“;

**27)** paragrahvi 7 täiendatakse lõigetega 2<sup>1</sup>–2<sup>3</sup> järgmises sõnastuses:

„(2<sup>1</sup>) Käesoleva paragrahvi lõikes 2 nimetatud turvameetmete rakendamisel arvestatakse:

- 1) süsteemi kaitsetarvet;
- 2) teenuse osutaja eriomaseid vajadusi ja turvanõudeid;
- 3) kaasaegseid ja asjakohasel juhul Euroopa ning rahvusvahelisi standardeid;
- 4) turvameetmete rakendamiskulusid;
- 5) turvameetmete rakendamise proportsionaalsust, mille hindamisel võetakse arvesse teenuse osutaja riskidele avatuse määra, teenuse osutaja suurust, küberintsidentide esinemise tõenäosust ja nende tõsidust, sealhulgas küberintsidentide ühiskondlikku ning majanduslikku mõju;
- 6) kõiki ohte hõlmavat lähenemisviisi, mille eesmärk on kaitsta süsteeme ja nende süsteemide füüsilist keskkonda küberintsidentide eest.

(2<sup>2</sup>) Käesoleva paragrahvi lõike 2 punktis 6 nimetatud tarneahela turvalisusega seotud turvameetmete asjakohasust kaaludes võtab teenuse osutaja arvesse:

- 1) koostööpartnerile eriomaseid nõrkusi, koostööpartneri toote üldist kvaliteeti ja küberturvalisuse tavadid, sealhulgas toote turvalise arenduse korda;
- 2) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 22 lõike 1 kohaselt korraldatud kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamiste tulemusi.

(2<sup>3</sup>) Kui teenuse osutaja tuvastab, et ta ei rakenda käesoleva paragrahvi lõikes 2 sätestatud turvameetmeid, võtab ta põhjendamatu viivitusega kõik vajalikud, asjakohased ja proportsionaalsed parandusmeetmed turvameetmete rakendamiseks.“;

**28)** paragrahvi 7 täiendatakse lõikega 6 järgmises sõnastuses:

„(6) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 tähenduses Euroopa Komisjoni rakendusakti vastu võtmisel, millega sätestatakse tehnilised, meetodilised ja

vajaduse korral valdkondlikud nõuded turvameetmete rakendamiseks teenuse osutaja poolt, lähtub rakendusaktis nimetatud teenuse osutaja rakendusaktiga kehtestatud nõuetest osas, mis on vastuolus käesoleva paragrahvi lõike 5 alusel kehtestatud määruses sätestatuga.“;

**29)** paragrahvi 8 lõiget 1 täiendatakse pärast tekstiosa „Teenuse osutaja“ tekstiosaga „, välja arvatud julgeolekuasutus,“;

**30)** paragrahvi 8 lõike 2 punktides 1 ja 4 asendatakse arv „1“ arvuga „14“;

**31)** paragrahvi 8 lõiget 2 täiendatakse punktiga 6 järgmises sõnastuses:

„6) tegemist on Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 23 lõike 11 alusel vastu võetud Euroopa Komisjoni rakendusaktis sätestatud olulise küberintsidendiga.“;

**32)** paragrahvi 8 lõige 4 tunnistatakse kehtetuks;

**33)** paragrahvi 8 täiendatakse lõigetega 4<sup>1</sup> ja 4<sup>2</sup> järgmises sõnastuses:

„(4<sup>1</sup>) Olulise mõjuga küberintsidendi teavituses esitatakse võimaluse korral järgmised andmed:

1) teave olulise mõjuga küberintsidendi sisu ja toimumise põhjuse kohta, sealhulgas asjakohasel juhul teave turvarikkemärgi kohta;

2) hinnang olulise mõjuga küberintsidendile, sealhulgas selle tõsidusele ja mõjule;

3) teave olulise mõjuga küberintsidendi piiriülese mõju kohta;

4) teave tegevuste kohta olulise mõjuga küberintsidendi lahendamiseks.

(4<sup>2</sup>) Riigi Infosüsteemi Ameti taotlusel esitab teenuse osutaja vahearuande olulise mõjuga küberintsidendi lahendamise seisu kohta. Vahearuandes esitatakse käesoleva paragrahvi lõikes 4<sup>1</sup> nimetatud andmed ja asjakohasel juhul Riigi Infosüsteemi Ameti taotluses küsitud täiendav teave.“;

**34)** paragrahvi 8 lõige 5 muudetakse ja sõnastatakse järgmiselt:

„(5) Teenuse osutaja on kohustatud teavitama mõistliku aja jooksul isikut, keda olulise mõjuga küberintsident või oluline küberoht võib mõjutada, või avalikkust, kui mõjutatud isikuid ei ole võimalik eraldi teavitada. Teavituses annab teenuse osutaja võimalusel teada olulisest küberohust ja meetmetest või parandusmeetmetest, mida mõjutatud isik saab olulisele küberohule reageerimiseks võtta.“;

**35)** paragrahvi 8 lõige 7 muudetakse ja sõnastatakse järgmiselt:

„(7) Teenuse osutaja on olulise mõjuga küberintsidendi teavituse esitamisest kohustatud edastama ühe kuu jooksul Riigi Infosüsteemi Ametile raporti, mis sisaldab informatsiooni

küberintsidendi tekkepõhjuste, selle lahendamiseks kulunud aja ja rakendatud abinõude ning küberintsidendi mõju, sealhulgas asjakohasel juhul piiriülese mõju kohta. Kui raporti esitamise hetkel jätkub olulise mõjuga küberintsidendi lahendamine, on esitatud raport käsitletav vahearuaandena ja teenuse osutaja esitab ühe kuu jooksul raporti pärast olulise mõjuga küberintsidendi lahendamist.“;

**36)** paragrahvi 8 täiendatakse lõikega 8<sup>1</sup> järgmises sõnastuses:

„(8<sup>1</sup>) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 23 lõike 11 tähenduses Euroopa Komisjoni rakendusakti vastu võtmisel, milles kehtestatakse nõuded küberintsidendi, sealhulgas olulise mõjuga küberintsidendi, kohta esitatava teavituse või raporti korra ja vormi kohta, lähtutakse nimetatud rakendusaktis sätestatud nõuetest.“;

**37)** paragrahvi 8 lõige 9 tunnistatakse kehtetuks;

**38)** paragrahvi 8 täiendatakse lõikega 10 järgmises sõnastuses:

„(10) Julgeolekuasutuses teavitab küberintsidendist asjakohast julgeolekuasutust, arvestades käesolevas paragrahvis sätestatud nõudeid.“;

**39)** seadust täiendatakse §-ga 8<sup>1</sup> järgmises sõnastuses:

#### **„§ 8<sup>1</sup>. Vabatahtlik teavitamine**

(1) Riigi Infosüsteemi Ametile võib:

- 1) teenuse osutaja teavitada küberintsidendist, nõrkusest ja küberohust;
- 2) muu isik kui teenuse osutaja teavitada olulise mõjuga küberintsidendist, nõrkusest ja küberohust.
- (2) Potentsiaalsest nõrkusest või nõrkusest teavitav füüsiline või juriidiline isik võib esitada teate anonüümselt. Anonüümselt esitatud teate esitaja isik on asutusesiseseks kasutamiseks mõeldud teave.
- (3) Käesoleva paragrahvi lõikes 1 alusel esitatud teavituse lahendamisel lähtub Riigi Infosüsteemi Amet käesoleva seaduse §-dest 8 ja 12.“;

**40)** paragrahvid 10 ja 11 tunnistatakse kehtetuks;

**41)** paragrahvi 12 täiendatakse lõigetega 3<sup>1</sup> ja 3<sup>2</sup> järgmises sõnastuses:

„(3<sup>1</sup>) Riigi Infosüsteemi Amet annab olulise mõjuga küberintsidendi teavituse saamisel võimaluse korral 24 tunni jooksul teavitanud teenuse osutajale vastuse, mis sisaldab esialgset tagasisidet olulise mõjuga küberintsidendile ja teavitanud üksuse taotluse korral ka suuniseid olulise mõjuga küberintsidendi lahendamise meetmete kohta.

(3<sup>2</sup>) Riigi Infosüsteemi Amet võib eelistada küberintsidendi lahendamisel käesoleva seaduse paragrahvi 8 alusel esitatud teavituse lahendamist käesoleva seaduse paragrahvi lõikes 8<sup>1</sup> alusel esitatud teavituse lahendamisele.“;

**42)** paragrahvi 12 lõige 4 muudetakse ja sõnastatakse järgmiselt:

„(4) Riigi Infosüsteemi Ametil on õigus välisriigile või Euroopa Liidu Küberturvalisuse Ametile või muule organisatsioonile edastada küberintsidendi ennetamise ja lahendamise seotud teavet käesoleva seaduse §-s 5 sätestatud ülesannete või Euroopa Liidu õigusest tuleneva kohustuse täitmiseks või välislepinguga ettenähtud juhtudel ja korras, kui edastatav teave ei kahjusta riigi julgeolekut või kriminaalmenetlust. Nimetatud teabe edastamise kohustus on ennekõike siis, kui olulise mõjuga küberintsident on seotud kahe või enama Euroopa Liidu liikmesriigiga, mille korral tuleb asjakohane olulise mõjuga küberintsidendi kohta käiv teave edastada puudutatud välisriigile ja Euroopa Liidu Küberturvalisuse Ametile.“;

**43)** paragrahvi 12 täiendatakse lõikega 4<sup>1</sup> järgmises sõnastuses:

„(4<sup>1</sup>) Riigi Infosüsteemi Amet esitab Euroopa Liidu Küberturvalisuse Ametile iga kolme kuu tagant koondaruande, mis sisaldab anonüümseid koondandmeid olulise mõjuga küberintsidentide, küberintsidentide ja küberohtude kohta.“;

**44)** paragrahvi 12 lõikest 5 jäetakse välja tekstiosa „või digitaalse teenuse osutaja“;

**45)** seadust täiendatakse §-ga 12<sup>1</sup> järgmises sõnastuses:

**„§ 12<sup>1</sup>. Ulatusliku küberintsidendi ja kriisi ennetus ning lahendamine**

(1) Ulatusliku küberintsidendi ja kriisi ennetusele ning lahendamisele kohaldatakse käesoleva seaduse §-i 12 ja kriisi ennetamise ning lahendamise seotud muid valdkondlikke seadusi.

(2) Riigi Infosüsteemi Amet:

1) koostab ja võtab vastu ulatuslike küberintsidentide ning kriiside lahendamise kava (edaspidi *kava*), mis arvestab Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 9 lõikes 4 olevaid nõudeid;

2) teavitab kava vastu võtmisest või vastu võetud kavaga seotud muudatuste tegemisest kolme kuu jooksul Euroopa Komisjonile ja Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikule (EU-CyCLONe) asjakohase teabe, mis on seotud nimetatud kavaga.

(3) Kava võib koostada muu õigusakti alusel koostatava dokumendi osana.“;

**46)** paragrahvi 13 lõige 1 muudetakse ja sõnastatakse järgmiselt:

„(1) Küberintsidentide register (edaspidi *register*) on Riigi Infosüsteemi Ameti peetav andmekogu, kuhu kantakse küberintsidendi toimumist, küberohte ja nõrkusi kirjeldavad andmed

eesmärgiga pidada küberintsidentide, küberohtude ning nõrkuste üle arvestust ja analüüsida registrisse esitatud teavet nende ennetamiseks või lahendamiseks, ohuteadete edastamiseks ning järelevalvetoimingute tegemiseks.“;

47) paragrahvi 13 täiendatakse lõikega 4 järgmises sõnastuses:

„(4) Käesoleva paragrahvi lõikes 3 nimetatud määruses täpsustatakse registri andmekoosseis ja andmeandjad, registrile juurdepääs, registrisse kantud andmete säilitustähtaeg ning registriga seotud muud korralduslikud nõuded.“;

48) paragrahvi 13<sup>1</sup> tekstist jäetakse välja tekstiosa „, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 07.06.2019, lk 15–69),“;

49) seadust täiendatakse §-ga 13<sup>3</sup> järgmises sõnastuses:

**„§ 13<sup>3</sup>. Euroopa küberturvalisuse sertifitseerimise kavade kasutamine**

(1) Vabariigi Valitsus võib määrusega kohustada teenuse osutajat järgima käesoleva seaduse §-s 7 sätestatud nõuetele vastavuse tõenduseks teatavate IKT-toodete, IKT-teenuste ja IKT-protsesside kasutamist, mis on sertifitseeritud Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 49 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava alusel ning mis on:

- 1) töötatud välja teenuse osutaja poolt; või
- 2) hangitud kolmandalt isikult.

(2) Käesoleva paragrahvi lõike 1 kohase Vabariigi Valitsuse määruse andmisel täpsustatakse samas määruses kohustuse sisu, ulatust, täitmise tähtaega ja täpsemaid nõudeid.

(3) Erisusena käesoleva paragrahvi lõikest 1 lähtub teenuse osutaja Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 24 lõike 2 alusel vastu võetud Euroopa Komisjoni delegeeritud õigusaktist, kui asjakohane delegeeritud õigusakt on vastu võetud.“;

50) paragrahvi 14 lõige 2 tunnistatakse kehtetuks;

51) paragrahvi 14 lõiget 5 täiendatakse teise lausega sõnastuses „Haldusjärelevalvet teostavale julgeolekuasutusele kohaldatakse käesoleva paragrahvi lõigetes 6–12 ja käesoleva seaduse §-s 17 sätestatut.“;

52) paragrahvi 14 täiendatakse lõigetega 6–14 järgmises sõnastuses:

„(6) Riigi Infosüsteemi Amet järelevalve tegemisel:

- 1) võib prioriseerida käesolevas seaduses sätestatud ülesannete täitmist, arvestades riski- või ohuproгноosi põhist lähenemist;
- 2) viib elutähtsa üksuse suhtes läbi riiklikku ja haldusjärelevalvet põhjaliku ennetava- või järelkontrollina;
- 3) viib olulise üksuse suhtes läbi riiklikku ja haldusjärelevalvet järelkontrollina, kui järelevalveasutus saab teada, et oluline üksus ei järgi käesolevas seaduses, ennekõike käesoleva seaduse §-des 7 ja 8, sätestatud nõudeid;
- 4) võib algatada järelevalvemenetluse omal algatusel.

(7) Riikliku ja haldusjärelevalve meetme kohaldamisel võetakse arvesse iga üksikjuhtumi asjaolusid, ennekõike:

- 1) rikkumise raskust ja rikutud nõuete olulisust;
- 2) rikkumise kestust;
- 3) asjaomase teenuse osutaja varasemaid asjassepuutuvaid rikkumisi;
- 4) põhjustatud varalise või mittevaralise kahju, sealhulgas rahalise või majandusliku kahju, mõju teistele teenustele;
- 5) rikkumisest mõjutatud isikute arvu;
- 6) rikkumise toimepanija tahtlust või hooletust;
- 7) turvameetmed, mida teenuse osutaja on võtnud varalise või mittevaralise kahju ennetamiseks või vähendamiseks;
- 8) kinnitatud tegevusjuhendite järgimise või kinnitatud sertifitseerimismehhanismide rakendamise seisu;
- 9) käesoleva paragrahvi lõigetes 1 ja 5 nimetatud järelevalveasutuse ning teenuse osutaja koostöö taset.

(8) Raskeks rikkumiseks käesoleva paragrahvi lõikes 7 punkti 1 tähenduses loetakse järgmised olukorrad:

- 1) tegemist on korduva rikkumisega;
- 2) teenuse osutaja on jätnud täitmata käesoleva seaduse § 8 lõikes 1 sätestatud kohustuse;
- 3) olulise mõjuga küberintsidendi korral jätab teenuse osutaja kasutusele võtmata turvameetmed olulise mõjuga küberintsidendi lahendamiseks;
- 4) käesoleva paragrahvi lõigetes 1 ja 5 nimetatud järelevalveasutuselt saadud siduvate juhiste järgi puuduste kõrvaldamata jätmine;
- 5) rikkumise tuvastamise järel käesoleva paragrahvi lõigetes 1 ja 5 nimetatud järelevalveasutuse tellitud auditi või riikliku või haldusjärelevalve takistamine;
- 6) valeandmete või lubamatult ebatäpsete andmete esitamine seoses käesoleva seaduse §-s 7 sätestatud turvameetmete rakendamisega ja §-s 8 sätestatud olulise mõjuga küberintsidendist teavitamisega.
- (9) Riigi Infosüsteemi Ametil on riikliku ja haldusjärelevalve läbi viimisel õigus teha:

- 1) teenuse osutaja suhtes kohapealset kontrolli ja kaugjärelevalvet lähtudes käesoleva paragrahvi lõike 6 punktidest 2–4, sealhulgas elutähtsa üksuse suhtes pistelist järelevalvet, mis võib olla muuhulgas ajendatud olulise mõjuga küberintsidendist või käesolevas seaduses, sama seaduse alusel kehtestatud või Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktis kehtestatud nõude rikkumisest;
  - 2) teenuse osutaja suhtes sihipäraseid turvaauditeid, mis põhinevad Riigi Infosüsteemi Ameti või auditeeritava teenuse osutaja tehtud riskihindamisel või muul kättesaadaval riskialasel teabel;
  - 3) vajaduse korral koostöös asjaomase teenuse osutajaga objektiivsetel, mittediskrimineerivatel, õiglastel ja läbipaistvatel riskihindamise kriteeriumidel põhinevaid turvalisuse kontrole;
  - 4) hoiatuse teenuse osutajale, kui teenuse osutaja rikub käesolevat seadust, käesoleva seaduse alusel või Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktis kehtestatud nõuet;
  - 5) ettekirjutuse, millega nõutakse ettekirjutuse saajalt lõpetada tegevus või praktika, mis rikub käesolevas seaduses, käesoleva seaduse alusel või Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktis kehtestatud nõuet, ja hoiduda sama tegevuse või praktika kasutamisest;
  - 6) ettekirjutuse, millega nõutakse ettekirjutuse saajalt käesoleva seaduse §-s 7 sätestatud ning selle alusel kehtestatud nõuetele või Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 võetud rakendusaktis kehtestatud nõuetele vastavust ning käesoleva seaduse §-s 8 sätestatud teavituse esitamist samas paragrahvis viidatud viisil ja etteantud tähtajal;
  - 7) ettekirjutuse, millega nõutakse ettekirjutuse saajalt käesoleva seaduse § 8 lõikes 5 sätestatud teavituse tegemist;
  - 8) ettekirjutuse, millega nõutakse ettekirjutuse saajalt turvaauditi tulemuse alusel tehtud soovitude rakendamist mõistliku aja jooksul;
  - 9) ettekirjutuse, millega nõutakse ettekirjutuse saajalt käesolevas seaduses, käesoleva seaduse alusel või Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktis kehtestatud nõude rikkumise asjaolude avalikustamist ettekirjutuses ette nähtud viisil;
  - 10) ettekirjutuse elutähtsale üksusele, millega nõutakse ettekirjutuse saajalt kindlaks määratud perioodiks määrata kindlaks vastavushaldur, kes jälgib, kas ettekirjutuse adressaat täidab käesoleva seaduse §-des 7 ja 8 ning nende alusel või Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktis kehtestatud nõuet.
- (10) Käesoleva paragrahvi lõike 9 punktis 2 nimetatud sihipärase turvaauditi:
- 1) võib Riigi Infosüsteemi Amet teha elutähtsa üksuse suhtes korrapäraselt;
  - 2) viib läbi sõltumatu organ või Riigi Infosüsteemi Amet;
  - 3) tulemused tehakse kättesaadavaks Riigi Infosüsteemi Ametile;

4) kulud kannab auditeeritav teenuse osutaja, välja arvatud juhul, kui Riigi Infosüsteemi Amet põhjendatult juhul otsustab teisiti.

(11) Elutähtsa üksuse suhtes käesoleva paragrahvi lõike 9 punktis 5 nimetatud ettekirjutus võib sisaldada ka küberintsidendi ennetamiseks või heastamiseks ette nähtud turvameetmeid ja nõudeid turvameetmete rakendamise tähtaja ning rakendamisest täitmise teavitamise kohta.

(12) Kui elutähtsa üksuse suhtes käesoleva paragrahvi lõike 9 punktides 4–6 ja 8 nimetatud järelevalve meede ei anna tulemust, määrab Riigi Infosüsteemi Amet elutähtsale üksusele täiendava tähtaja puuduste kõrvaldamiseks või Riigi Infosüsteemi Ameti esitatud nõuete täitmiseks.

(13) Kui elutähtis üksus ei kõrvalda puudusi või ei täida Riigi Infosüsteemi Ameti nõudeid käesoleva paragrahvi lõike 12 alusel määratud tähtajaks, on Riigi Infosüsteemi Ametil õigus nõuda ettekirjutusega:

1) elutähtsa üksuse kõigi või mõnede osutatavate asjaomaste teenuste või tegevuste sertifikaadi või loa ajutist peatamist loa väljastajalt, või vastava pädevuse olemasolul teha ise nimetatud toiminguid;

2) elutähtsa üksuse nõukogult või osanikelt juhatuse liikme volituste ajutist peatamist.

(14) Käesoleva paragrahvi lõike 13 punktides 1 ja 2 sätestatud meetmeid:

1) kohaldatakse seni, kuni kõnealune elutähtis üksus võtab kasutusele vajalikud meetmed puuduste kõrvaldamiseks või Riigi Infosüsteemi Ameti esitatud nõuete täitmiseks;

2) ei kohaldata keskvalitsuse avaliku halduse üksuse või kohaliku tasandi avaliku halduse üksuse suhtes, sealhulgas juhul, kui sama üksus on kvalifitseeritud usaldusteenuse osutaja.“;

**53)** paragrahvi 15 lõige 2 muudetakse ja sõnastatakse järgmiselt:

„(2) Käesoleva seaduse §-de 7 ja 8 ning nende alusel kehtestatud õigusaktide või Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktis kehtestatud nõuete täitmise üle riikliku järelevalve tegemisel võib korrakaitseorgan kohaldada lisaks käesoleva paragrahvi lõikes 1 nimetatud erimeetmetele ka korrakaitseseaduse §-des 52 ja 53 sätestatud riikliku järelevalve erimeedet korrakaitseseaduses sätestatud alusel ja korras.“;

**54)** paragrahvi 17<sup>1</sup> tekst muudetakse ja sõnastatakse järgmiselt:

„Riikliku ja haldusjärelevalvemenetluse käigus ettekirjutuse täitmata jätmise korral on asendustäitmise ja sunniraha seaduses sätestatud korras rakendatava sunniraha kohaldamise igakordne ülemmäär 7 000 000 eurot või kuni 1,4 protsenti teenuse osutaja omanikust ettevõtja eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.“;

**55)** seadust täiendatakse §-ga 17<sup>3</sup> järgmises sõnastuses:



### **„§ 17<sup>3</sup>. Vastastikune abi**

(1) Riigi Infosüsteemi Amet ning Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 8 alusel nimetatud pädevad asutused (edaspidi koos *järelevalveasutus*) teevad koostööd asjakohase teabe vahetamiseks ning vajaduse korral abistavad üksteist, kui teenuse osutaja osutab teenuseid mitmes Euroopa Liidu liikmesriigis või kui ta osutab teenuseid ühes või mitmes liikmesriigis, kuid tema süsteemid asuvad ühes või mitmes muus liikmesriigis.

(2) Järelevalveasutus annab teiselt järelevalveasutuselt saadud põhjendatud taotluse korral kõnealusele asutusele enda käsutuses olevate ressursidega proportsionaalset abi, et järelevalve- või täitemeetmeid saaks rakendada tulemuslikult, tõhusalt ja järjepidevalt. Vastastikune abi võib hõlmata eelkõige teabepäringuid ja järelevalvemeetmeid, sealhulgas taotlusi teha kohapealseid kontrolle, kaugjärelevalvet või sihipäraseid turvaauditeid.

(3) Käesoleva paragrahvi lõikes 1 olukorras võib Riigi Infosüsteemi Amet käesolevas paragrahvi lõikes 2 nimetatud abitaotluse esitada teise Euroopa Liidu liikmesriigi Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 8 alusel nimetatud pädevale asutusele.

(4) Riigi Infosüsteemi Amet võib teise Euroopa Liidu liikmesriigi Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 8 alusel nimetatud pädeva asutuse esitatud abitaotluse täitmisest keelduda, kui:

- 1) Riigi Infosüsteemi Amet ei ole pädev taotletavat abi andma;
- 2) taotletav abi ei ole proportsionaalne Riigi Infosüsteemi Ameti ülesannete suhtes; või
- 3) taotlus puudutab teavet või sisaldab tegevust, mis avalikustamise või elluviimise korral oleksid vastuolus riikliku julgeoleku, avaliku julgeoleku või riigikaitse oluliste huvidega.

(5) Enne abitaotluse rahuldamata jätmist konsulteerib Riigi Infosüsteemi Amet teiste asjaomaste pädevate asutustega ja ühe asjaomase liikmesriigi taotluse korral ka Euroopa Komisjoni ning Euroopa Liidu Küberturvalisuse Ametiga.

(6) Arvestades käesolevas seaduses nimetatud järelevalvemeetmeid võib Riigi Infosüsteemi Amet rakendada ühiseid järelevalve- ja täitemeetmeid, millesse on kaasatud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 8 alusel nimetatud pädeva asutuse töötajad või ametnikud. Järelevalveasutused lepivad omavahel kokku ühistegevuse korra ja protseduurid.

(7) Kui Eesti saab vastastikuse abi taotluse seoses digitaalse teenuse osutajaga, siis Riigi Infosüsteemi Amet võib võtta taotluses nimetatud Eesti territooriumil teenuseid osutava digitaalse teenuse osutaja suhtes või digitaalse teenuse osutaja suhtes, kellel on Eesti Vabariigi territooriumil süsteem, esitatud taotluse ulatuses asjakohaseid järelevalve- ja täitemeetmeid.“;

56) seadust täiendatakse 4<sup>1</sup>. peatükiga järgmises sõnastuses:

### **„4<sup>1</sup>. peatükk**

#### **Koostöö, teabevahetus ja vastastikune hindamine**

## **§ 17<sup>4</sup>. Riigi Infosüsteemi Ameti ja julgeolekuasutuse ülesanded koostöö tegemisel**

(1) Riigi Infosüsteemi Amet ja julgeolekuasutus teeb oma ülesannete täitmise käigus koostööd:

- 1) isikuandmete kaitse seaduse tähenduses õiguskaitseasutustega;
- 2) isikuandmete kaitse järelevalveasutustega;
- 3) Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 300/2008 kohaste riiklike asutustega;
- 4) Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme ja millega luuakse Euroopa Liidu Lennundusohutusamet ning millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 2111/2005, (EÜ) nr 1008/2008, (EL) nr 996/2010, (EL) nr 376/2014 ja Euroopa Parlamendi ja nõukogu direktiive 2014/30/EL ning 2014/53/EL ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 552/2004 ja (EÜ) nr 216/2008 ning nõukogu määrus (EMÜ) nr 3922/91 (ELT L 212, 22.08.2018, lk 1–122), kohaste riiklike asutustega;
- 5) Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 kohaste järelevalveasutustega;
- 6) Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1–79), kohaste pädevate asutustega;
- 7) Tarbijakaitse ja Tehnilise Järelevalve Ametiga;
- 8) julgeolekuasutusega;
- 9) teenuse osutajate sektoripõhiste või -vaheliste kogukondadega, sealhulgas vajadusel vahetades nendega teavet arvestades käesoleva seaduse §-s 17<sup>5</sup> sätestatud nõudeid;
- 10) muude Euroopa Liidu õigusaktide kohaste pädevate asutustega.

(2) Riigi infosüsteemi Amet teeb igakülgset koostööd elutähtsat teenust korraldavate asutuse või tema hädaolukorra seaduse § 37 lõike 5 alusel määratud asutuse, Päästeameti ja Riigikantseleiga ning vahetab teavet elutähtsa teenuse osutajatega edastatud olulise mõjuga küberintsidentide, küberriskide, -ohtude ja -intsidentide kohta ning elutähtsa teenuse osutajatena käsitatavaid elutähtsaid üksusi mõjutavate muude kui küberriskide, -ohtude ja -intsidentide kohta ning selliste riskide, ohtude ja küberintsidentide lahendamiseks võetud meetmete kohta. Lisaks teavitab Riigi Infosüsteemi Amet nimetatud asutust, kui Riigi Infosüsteemi Amet võtab elutähtsa teenuse osutaja suhtes riikliku või haldusjärelevalve käigus kasutusele järelevalve meetet. Sama asutus võib asjakohasel juhul taotleda Riigi Infosüsteemi Ametilt riikliku või haldusjärelevalve menetluses ette nähtud järelevalve meetme kasutamist elutähtsa teenuse osutaja suhtes.

(3) Riigi Infosüsteemi Amet teavitab Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2554 artikli 32 lõike 1 kohaselt järelevaatamise foorumit, kui Riigi Infosüsteemi Amet kasutab riikliku järelevalve käigus järelevalve meetet, et tagada nimetatud määruse artikli 31 kohaselt kriitilise tähtsusega kolmandast isikust IKT-teenuse osutajana käsitatava ja käesoleva seaduse kohaldamisalasse kuuluva teenuse osutaja vastavust käesolevas seaduses või käesoleva seaduse alusel kehtestatud nõuetele.

(4) Riigi Infosüsteemi Amet ja käesoleva paragrahvi lõike 1 punktides 5-8 nimetatud asutused vahetavad korrapäraselt asjakohast teavet, sealhulgas asjaomaste küberintsidentide ja -ohtude kohta.

(5) Riigi Infosüsteemi Amet täidab pädeva asutusena Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 8 lõike 1 tähenduses sidepidamisfunktsiooni tagamaks Eesti ametiasutuste piiriülene koostöö küberturvalisuse valdkonnas teiste Euroopa Liidu liikmesriikide asjaomaste pädevate asutustega ning asjakohasel juhul ka Euroopa Komisjoni ja Euroopa Liidu Küberturvalisuse Ametiga.

(6) Teabe vahetamisel tagatakse edastatava teabe turvalisus ja asjakohasel juhul kasutatakse kokku lepitud teabevahetuse protokolle, sealhulgas fooriprotokolle.

### **§ 17<sup>5</sup>. Küberturvalisuse alase teabevahetuse kokkulepped**

(1) Teenuse osutajad kui ka muud isikud võivad omavahel vabatahtlikult vahetada asjakohast küberturvalisuse alast teavet, sealhulgas teavet, mis on seotud küberohtude, nõrkuste, meetodite ja menetluste, rikkeindikaatorite, kahjulike taktikate, ohusubjekti spetsiifilise teabe, küberturvalisuse hoiatuste ning soovitustega küberturvalisuse vahendite konfiguratsiooni kohta küberrünnete tuvastamiseks, kui selline teabevahetus:

1) toimub küberintsidentide ennetamise, tuvastamise, lahendamise või nende tagajärgede leevendamise eesmärgil; või

2) aitab tõsta küberturvalisuse taset, eelkõige küberohtude alase teadlikkuse suurendamise ja kõnealuste ohtude leviku piiramise või takistamise kaudu ning toetades mitmesuguseid kaitsevõimalusi, nõrkuste vähendamist ja avalikustamist, ohu tuvastamise, ohjamise ning ennetamise meetodeid, leevendusstrateegiaid, lahendamis- ja taastamisetappe ning avaliku ja erasektori üksuste koostöös toimuvat küberohtude uurimist.

(2) Käesolevas paragrahvi lõikes 1 nimetatud teabevahetus toimub küberturvalisuse alase teabevahetuse kokkuleppe (edaspidi *teabevahetuse kokkulepe*) alusel. Teabevahetuse kokkuleppeid võib olla rohkem kui üks.

(3) Teabevahetuse kokkuleppes võib täpsustada teabevahetuse korraldusega seotud tegevuste sisu, sealhulgas sihtotstarbeliste info- ja kommunikatsioonitehnoloogia platvormide ja automatiseerimisvahendite kasutamist kui ka muud sisu ning tingimusi, arvestades jagatava teabe tundlikkust.

(4) Riigi Infosüsteemi Amet võib enda poolt teabevahetuse kokkuleppe alusel kättesaadavaks tehtud teabele seada tingimusi, kui teabevahetuse kokkuleppes osaleb keskvalitsuse avaliku halduse üksus või kohaliku tasandi avaliku halduse üksus.

(5) Teenuse osutaja teavitab Riigi Infosüsteemi Ametit, kui teenuse osutaja on ühinenud teabevahetuse kokkuleppega või kui teabevahetuse kokkuleppest taganemine on jõustunud.

### **§ 17<sup>6</sup>. Vastastikune hindamine**

(1) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 19 sätestatud vastastikusel hindamisel (edaspidi *vastastikune hindamine*) osalemine on vabatahtlik.

(2) Vastastikuses hindamises osalemise korral lähtutakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 19 lõigetes 1 ja 6 nimetatud vastastikuse hindamise metoodikast, korralduslikest aspektidest ning tegevusjuhenditest, kui need on välja töötatud.

(3) Vastastikust hindamist teostavad küberturvalisuse valdkonna eksperdid, arvestades käesoleva paragrahvi lõikes 2 viidatud metoodikas sätestatud kriteeriume.

(4) Justiits- ja Digiministerium või tema volitatud asutus:

1) määrab kindlaks teise Euroopa Liidu liikmesriigi suhtes teostatavas vastastikuses hindamises Eesti Vabariigist osalevad küberturvalisuse valdkonna eksperdid;

2) teavitab vastastikuses hindamises osalevaid Euroopa Liidu liikmesriike, koostöörühma, Euroopa Komisjoni ning Euroopa Liidu Küberturvalisuse Ametit käesoleva paragrahvi lõike 4 punkti 1 alusel määratud ekspertidega seotud huvide konflikti ohust enne vastastikuse hindamise toimumist;

3) võib põhjendatud juhul esitada vastuväite Eesti Vabariigi suhtes hindamist läbi viiva teise Euroopa Liidu liikmesriigi küberturvalisuse valdkonna eksperdi määramise kohta ja esitada see vastuväide asjakohasele liikmesriigile;

4) määrab kindlaks vastastikuses hindamises hinnatavate aspektide sisu ja ulatuse arvestades Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 19 lõigetes 1 ning 3 olevaid nõudeid, ja teavitab nendest vastastikuses hindamises osalevatele Euroopa Liidu liikmesriikidele enne vastastikuse hindamise alustamist, kui vastastikuses hindamises hinnatakse Eesti Vabariiki;

5) võib enne vastastikuse hindamise toimumist koordineerida vastastikuses hindamises Eesti Vabariigi suhtes hinnatavate aspektide enesehindamist arvestades Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 19 lõike 5 alusel kehtestatud metoodikat, ning esitab enesehindamise tulemused Eesti Vabariigi suhtes hindamist läbi viivatele Euroopa Liidu liikmesriikide küberturvalisuse valdkonna ekspertidele;

6) edastab Eesti Vabariiki hinnatavale Euroopa Liidu liikmesriikide määratud küberturvalisuse valdkonna ekspertidele hindamiseks vajaliku teabe;

7) võib esitada käesoleva paragrahvi lõike 6 punktis 4 nimetatud taotluse;

8) võib koordineerida ja esitada märkusi Eesti Vabariigi suhtes koostatud aruande kavandi kohta;

9) võib vajadusel esitada koostöörühmale ja Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 15 nimetatud riiklike küberturbe intsidentide lahendamise üksuste võrgustikule Eesti Vabariigi suhtes tehtud vastastikuse hindamise aruande;

10) võib Eesti Vabariigi suhtes tehtava vastastikuse hindamise aruande või selle toimetatud versiooni teha üldsusele kättesaadavaks.

(5) Käesoleva paragrahvi lõike 4 punktis 6 nimetatud teabe edastamisel arvestatakse:

1) vastastikuses hindamises hinnatavaid aspekte ja ulatust;

2) juurdepääsupiiranguga teabe ja salastatud teabe kaitset;

3) Eesti Vabariigi, sh riigi julgeoleku huve; ja

4) riigi julgeoleku suhtes kehtivaid õigusakte.

(6) Vastastikuse hindamise käigus:

- 1) võib toimuda kohapealseid või virtuaalseid külastusi ja teabevahetust väljaspool hinnatavat tegevuskohta;
- 2) saadavat teavet kasutatakse üksnes vastastikuse hindamise eesmärgil;
- 3) osalevad küberturvalisuse valdkonna eksperdid hoiavad kolmandate isikute eest saladuses neile vastastikuse hindamise käigus teatavaks saadud teavet, kui seadus ei sätesta samaväärset saladuses hoidmise kohustust;
- 4) hinnatud aspektid ei kuulu kõnealuses riigis enam vastastikusele hindamisele kahe aasta jooksul pärast vastastikuse hindamise lõppemist, välja arvatud juhul, kui seda taotleb Eesti Vabariik või nii lepatakse kokku pärast koostöörühma ettepanekut;
- 5) osalevad küberturvalisuse eksperdid koostavad aruandeid vastastikuse hindamise tulemuste ja järelduste kohta;
- 6) koostatud aruanded sisaldavad soovitusi vastastikuse hindamisega hõlmatud aspektide parandamiseks.“;

57) paragrahv 18 tunnistatakse kehtetuks;

58) seadust täiendatakse §-dega 18<sup>2</sup>–18<sup>6</sup> järgmises sõnastuses:

**„§ 18<sup>2</sup>. Seaduse nõuete rikkumine elutähtsa üksuse poolt**

(1) Käesoleva seaduse § 7 lõigetes 1, 2, 2<sup>1</sup>, 2<sup>2</sup>, 3, 5 ja 6 või § 8 lõigetes 1, 1<sup>1</sup> ja 7 sätestatud nõuete rikkumise eest füüsilisest isikust elutähtsa üksuse poolt, kui puudub käesoleva seaduse §-s 18<sup>5</sup> sätestatud väärteokoosseis –

karistatakse rahatrahviga kuni 10 000 000 eurot.

(2) Sama teo eest, kui selle on toime pannud juriidilisest isikust elutähtis üksus –

karistatakse rahatrahviga kuni 10 000 000 eurot või kuni 2 protsenti elutähtsa üksuse omanikust ettevõtja eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.

**§ 18<sup>3</sup>. Seaduse nõuete rikkumine olulise üksuse poolt**

(1) Käesoleva seaduse § 7 lõigetes 1, 2, 2<sup>1</sup>, 2<sup>2</sup>, 3, 5 ja 6 või § 8 lõigetes 1, 1<sup>1</sup> ja 7 sätestatud nõuete rikkumise eest füüsilisest isikust olulise üksuse poolt, kui puudub käesoleva seaduse §-s 18<sup>5</sup> sätestatud väärteokoosseis –

karistatakse rahatrahviga kuni 7 000 000 eurot.

(2) Sama teo eest, kui selle on toime pannud juriidilisest isikust oluline üksus –

karistatakse rahatrahviga kuni 7 000 000 eurot või kuni 1,4 protsenti olulise üksuse omanikust ettevõtja eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.

**§ 18<sup>4</sup>. Teenuse osutaja juhtorgani või juhtorgani liikme poolne nõuete rikkumine**

Käesoleva seaduse §-s 6<sup>1</sup> nõuete rikkumise eest –  
karistatakse rahatrahviga kuni 300 trahviühikut.

#### **§ 18<sup>5</sup>. Piiriüleste elektrivoogudega seotud üksuse poolne nõuete rikkumine**

(1) Euroopa Komisjoni delegeeritud määruse (EL) 2024/1366 artikli 2 lõikes 1 nimetatud füüsilisest isikust üksuse poolt samas määruses sätestatud nõuete rikkumise eest –  
karistatakse rahatrahviga kuni 10 000 000 eurot.

(2) Sama teo eest, kui selle on toime pannud Euroopa Komisjoni delegeeritud määruse (EL) 2024/1366 artikli 2 lõikes 1 nimetatud juriidilisest isikust üksus –  
karistatakse rahatrahviga kuni 10 000 000 eurot või kuni 2 protsenti üksuse omanikust ettevõtja eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.

#### **§ 18<sup>6</sup>. Piiriüleste elektrivoogudega seotud üksuse seadusliku esindaja poolne nõuete rikkumine**

(1) Euroopa Komisjoni delegeeritud määruse (EL) 2024/1366 artikli 15 lõike 1 alusel nimetatud füüsilisest isikust seadusliku esindaja poolt samas määruses sätestatud nõuete rikkumise eest –  
karistatakse rahatrahviga kuni 300 trahviühikut.

(2) Sama teo eest, kui selle on toime pannud Euroopa Komisjoni delegeeritud määruse (EL) 2024/1366 artikli 15 lõike 1 alusel nimetatud füüsilisest isikust seadusliku esindaja –  
karistatakse rahatrahviga kuni 32 000 eurot.“;

**59)** paragrahvi 19 lõiked 1 ja 2 muudetakse ja sõnastatakse järgmiselt:

„(1) Käesoleva seaduse §-des 18<sup>2</sup>–18<sup>6</sup> sätestatud väärtegade kohtuväline menetleja on Riigi Infosüsteemi Amet.

(2) Kui käesoleva seaduse §-des 18<sup>2</sup> ja 18<sup>3</sup> sätestatud väärtegu on seotud isikuandmete töötlemise nõuete rikkumisega, kohaldatakse vääртеomenetluse puhul isikuandmete kaitse seadust.“;

**60)** paragrahvi 19 täiendatakse lõikega 4 järgmises sõnastuses:

„(4) Käesoleva seaduse §-des 18<sup>2</sup>, 18<sup>3</sup> ja 18<sup>5</sup> sätestatud väärtegade aegumistähtaeg on kolm aastat.“;

**61)** paragrahv 20 muudetakse ja sõnastatakse järgmiselt:

#### **„§ 20. Riigi Infosüsteemi Ametiga seotud ülesanded**

(1) Riigi Infosüsteemi Amet tuvastab käesoleva seaduse § 3 lõikes 3 nimetatud teenuse osutajad kuue kuu jooksul alates käesoleva seaduse § 3 lõike 3<sup>1</sup> jõustumisest.

(2) Riigi Infosüsteemi Amet teeb käesoleva seaduse § 3 lõike 3<sup>3</sup> punktides 1 ja 2 nimetatud teavitused kuue kuu jooksul alates viidatud punktide jõustumisest.

(3) Riigi Infosüsteemi Amet võib Euroopa Komisjoni taotlusel teatada kuue kuu jooksul Euroopa Komisjoni käesoleva seaduse § 3 lõike 3<sup>3</sup> punktis 2 osutatud teenuse osutajate nimed alates viidatud punkti jõustumisest.

(4) Riigi Infosüsteemi Amet nõuab digitaalse teenuse osutajatelt käesoleva seaduse § 4 lõikes 1 nimetatud teabe esitamist hiljemalt kolme kuu jooksul alates käesoleva seaduse § 2 lõike 7<sup>4</sup> jõustumisest.

(5) Riigi Infosüsteemi Amet edastab käesoleva seaduse § 12 lõikes 4<sup>1</sup> alusel tehtava esimese koondaruande kolme kuu jooksul alates viidatud lõike jõustumisest.“;

**62)** seaduse normitehniline märkus muudetakse ja sõnastatakse järgmiselt:

„Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152).“.

## **§ 2. E-identimise ja e-tehingute usaldusteenuste seaduse muutmine**

E-identimise ja e-tehingute usaldusteenuste seaduse § 4 tunnistatakse kehtetuks.

## **§ 3. Eesti Rahvusringhäälingu seaduse muutmine**

Eesti Rahvusringhäälingu seaduses tehakse järgmised muudatused:

1) paragrahvi 5 lõige 2<sup>1</sup> tunnistatakse kehtetuks;

2) paragrahvi 34 lõige 4<sup>1</sup> tunnistatakse kehtetuks.

## **§ 4. Elektroonilise side seaduse muutmine**

Elektroonilise side seaduses tehakse järgmised muudatused:

1) paragrahv 87<sup>2</sup> tunnistatakse kehtetuks;

2) paragrahvi 100<sup>3</sup> lõige 3 tunnistatakse kehtetuks;

3) paragrahvi 100<sup>4</sup> lõige 2 tunnistatakse kehtetuks;

4) paragrahvi 100<sup>5</sup> lõige 2 tunnistatakse kehtetuks;

5) paragrahvi 133 lõige 5 tunnistatakse kehtetuks;

6) paragrahv 170<sup>1</sup> tunnistatakse kehtetuks;

7) paragrahvi 188 lõige 8 tunnistatakse kehtetuks.

## **§ 5. Hädaolukorra seaduse muutmine**

Hädaolukorra seaduses tehakse järgmised muudatused:

1) paragrahvi 38 lõike 1<sup>3</sup> punkt 3 muudetakse ja sõnastatakse järgmiselt:

„3) täitma käesoleva seaduse § 37 lõike 2 alusel, §-s 41 ja muudes õigusaktides elutähtsa teenuse toimepidevuse tagamiseks sätestatud nõudeid, arvestades, et käesoleva seaduse §-s 41 ning küberturvalisuse seaduses sätestatud nõuete ja kohustuse täitmise tähtaeg ei oleks pikem kui viis aastat elutähtsa teenuse osutajaks määramisest arvates.“;

2) paragrahvi 38 lõikes 1<sup>4</sup> asendatakse tekstiosa „§-s 41“ tekstiosaga „küberturvalisuse seaduses“;

3) paragrahvi 41 lõige 1 tunnistatakse kehtetuks.

## **§ 6. Käibemaksuseaduse muutmine**

Käibemaksuseaduse § 4 lõikes 1<sup>2</sup> asendatakse sõna „küberturvalisuse“ sõnaga „tarbijakaitse“.

## **§ 7. Lennundusseaduse muutmine**

Lennundusseaduses tehakse järgmised muudatused:

1) paragrahv 59<sup>1</sup> tunnistatakse kehtetuks;

2) paragrahvi 60<sup>1</sup> lõige 5 tunnistatakse kehtetuks;

3) paragrahvi 60<sup>56</sup> lõige 3 tunnistatakse kehtetuks.

## **§ 8. Raudteeseaduse muutmine**



Raudteeseaduses tehakse järgmised muudatused:

- 1) paragrahv 8 tunnistatakse kehtetuks;
- 2) paragrahvi 143 lõike 1 punkt 6 tunnistatakse kehtetuks;
- 3) paragrahvi 143 lõige 8 tunnistatakse kehtetuks;
- 4) paragrahvi 148 tekstist jäetakse välja tekstiosa „, Riigi Infosüsteemide Amet“.

### **§ 9. Sadamaseaduse muutmine**

Sadamaseaduses tehakse järgmised muudatused:

- 1) paragrahvi 13 lõige 4 tunnistatakse kehtetuks;
- 2) paragrahvi 42 lõige 5 tunnistatakse kehtetuks.

### **§ 10. Tervishoiuteenuste korraldamise seaduse muutmine**

Tervishoiuteenuste korraldamise seaduses tehakse järgmised muudatused:

- 1) paragrahvi 10 lõige 2 tunnistatakse kehtetuks;
- 2) paragrahvi 17 lõige 1<sup>2</sup> tunnistatakse kehtetuks;
- 3) paragrahvi 22 lõige 4<sup>2</sup> tunnistatakse kehtetuks;
- 4) paragrahvi 60 lõige 2 tunnistatakse kehtetuks.

### **§ 11. Seaduse jõustumine**

Käesolev seadus jõustub 2025. aasta 1. juulil.

Lauri Hussar  
Riigikogu esimees

Tallinn,

2025

Algatab Vabariigi Valitsus