JUSTIITS- JA DIGIMINISTEERIUM

MINISTRI MÄÄRUS 22.01.2026 nr 3

Majandus- ja kommunikatsiooniministri 25. aprilli 2011. a määruse nr 28 „Riigi Infosüsteemi Ameti põhimäärus“ muutmine

Määrus kehtestatakse Vabariigi Valitsuse seaduse § 42 lõike 1 alusel.

Majandus- ja kommunikatsiooniministri 25. aprilli 2011. a määruses nr 28 „Riigi Infosüsteemi Ameti põhimäärus“ tehakse järgmised muudatused:

1) paragrahvi 8 lõike 1 punkti 9 täiendatakse pärast sõna „piires“ tekstiosaga „„ sealhulgas rahvusvahelistes koostöövõrgustikes“;

2) paragrahvi 8 lõike 4 punkt 3 sõnastatakse järgmiselt:

„3) täidab küberturvalisuse seaduse § 5 tähenduses pädeva asutuse, ühtse kontaktpunkti, ulatuslike küberintsidentide ja kriiside ohjamise eest vastutava pädeva asutuse, küberintsidentide käsitlemise üksuse ja turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid ning koordineerib küberintsidentide käsitlemist;“;

3) paragrahvi 8 lõiget 4 täiendatakse punktiga 3^1 järgmises sõnastuses:

„3^1) osaleb oma pädevuse kohaselt 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), artiklis 14 nimetatud koostöörühma tegevuses, artiklis 16 nimetatud Euroopa küberkriisiga tegelevate kontaktasutuste võrgustiku töös ja küberturvalisuse seaduse §-s 5 nimetatud küberintsidentide käsitlemise riiklike üksuste võrgustiku töös“;

4) määruse 2. peatükki täiendatakse §-ga 9^1 järgmises sõnastuses:

„§ 9^1. Ameti töökorralduslikud ja muud kohustused

Amet:

1) tagab oma sidekanalite laialdase ja pideva kättesaadavuse, kasutades selleks mitmesuguseid töökindlaid vahendeid, mis võimaldavad tal teistega ja teistel temaga igal ajal ühendust võtta;
2) määrab kindlaks sidekanalid ning teeb need teatavaks oma sihtrühmadele ja koostööpartneritele;
3) tagab, et tema ametiruumid ja tööd toetavad infosüsteemid asuvad turvalises kohas ning et teenuste toimepidevuse eesmärgil on olemas ka varusüsteemid ja -tööruumid;
4) tagab sellise päringute haldamiseks ja suunamiseks sobiva infosüsteemi olemasolu, mis võimaldab ka töid tõhusalt üle anda;
5) tagab oma tegevuse konfidentsiaalsuse ja usaldusväärsuse;
6) tagab oma teenuste pideva kättesaadavuse eesmärgil piisava arvu töötajate ja ametnike olemasolu;
7) tagab oma töötajatele ja ametnikele asjakohase väljaõppe.“;

5) paragrahvi 13 lõike 1 punktis 1 asendatakse sõna „ülesannete“ tekstiosaga „„ küberintsidentide käsitlemise üksuse ja turvahaavatavuse koordineeritult avaldamise koordinaatori ülesannete“;

6) paragrahvi 13 täiendatakse lõigetega 1^1 – 1^4 järgmises sõnastuses:

„(1^1) Küberturvalisuse keskus täidab küberintsidentide käsitlemise üksuse ülesandeid järgmiselt:
1) tegeleb oma ülesannete piires vähemalt Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 I ja II lisas osutatud sektorite, allsektorite või viidatud liiki üksustega ja vastutab küberintsidentide käsitlemise eest kindla menetluse kohaselt;
2) osaleb küberturvalisuse seaduses sätestatud vastastikuses hindamises;
3) teeb koostööd teiste Euroopa Liidu liikmesriikide küberintsidentide käsitlemise üksustega;
4) võib teha koostööd kolmandate riikide küberintsidentide käsitlemise riiklike üksustega või samaväärsete asutustega, sealhulgas küberturvalisusalase abi andmiseks;
5) teeb koostööd teenuseosutajate sektoripõhiste või -vaheliste kogukondadega, sealhulgas vahetab vajaduse korral nendega teavet, arvestades küberturvalisuse seaduses küberturvalisusalase teabevahetuse kokkuleppe kohta sätestatud nõudeid;
6) korraldab küberohtude, turvahaavatavuste ja küberintsidentide seiret ning analüüsi riiklikul tasandil;
7) taotluse korral osutab asjaomastele teenuseosutajatele abi nende võrgu- ja infosüsteemide reaalajalise või reaalajalähedase seirega;
8) tagab küberohu, turvahaavatavuse ja küberintsidendi kohta varajase hoiatuse, hoiatuse ja teate edastamise ning teabe levitamise asjaomastele teenuseosutajatele, pädevatele asutustele ja muudele asjaomastele sidusrühmadele, võimaluse korral edastatakse varajane hoiatus, hoiatus ja teade reaalajalähedaselt;
9) lahendab küberintsidente ja asjakohasel juhul abistab asjaomaseid teenuseosutajaid;
10) kogub ja analüüsib digitaalkriminalistika andmeid, analüüsib järjepidevalt riske ja küberintsidente, ning tagab teadlikkuse küberturvalisuse olukorrast;
11) kontrollib potentsiaalselt olulise mõjuga turvahaavatavuse kindlakstegemiseks ennetavalt teenuseosutaja taotlusel teenuseosutaja võrgu- ja infosüsteemi;
12) osaleb küberintsidentide käsitlemise riiklike üksuste võrgustiku töös ja osutab teisele võrgustiku liikmele taotluse korral oma võimete ja pädevuse kohast abi;
13) täidab turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid;
14) aitab teenuseosutajatel ja asjaomastel sidusrühmadel kasutusele võtta nendega teabe turvaliseks vahetamiseks mõeldud vahendeid;
15) teeb vajaduse korral teenuseosutaja üldkasutatava võrgu- ja infosüsteemi ennetavat välist kontrolli, mille eesmärk on tuvastada haavatav või ebaturvaliselt seadistatud süsteem ja teavitada sellest asjaomast teenuseosutajat, tagades, et kontroll ei avalda negatiivset mõju teenuseosutaja teenuse toimimisele;

16) loob koostöösuhteid erasektori asjaomaste sidusrühmadega ning toetab koostöö hõlbustamiseks ühtsete või standardsete tavade ja liigitamissüsteemide kasutuselevõttu seoses küberintsidendi käsitlemise menetluse, kriisiohje ja turvahaavatavuse koordineeritud avaldamisega.

(1^2) Lõike 1^1 punktides 6–14 sätestatud ülesandeid võib riski- või ohuprognoosipõhise lähenemisviisi alusel prioriseerida.

(1^3) Küberturvalisuse keskus täidab turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid järgmiselt:
1) tegutseb usaldusväärse vahendajana, hõlbustades vajaduse korral turvahaavatavusest teavitava füüsilise või juriidilise isiku ja potentsiaalse turvahaavatavusega IKT-toote tootja või IKT-teenuse osutaja vahelist suhtlust, tegutsedes ükskõik kumma poole taotlusel;
2) teeb kindlaks teavitatud potentsiaalse turvahaavatavuse või turvahaavatavusega seotud üksuse ja võtab temaga ühendust;
3) abistab potentsiaalsest turvahaavatavusest ja turvahaavatavusest teavitavat füüsilist või juriidilist isikut;
4) peab läbirääkimisi avalikkuse turvahaavatavusest teavitamise tähtaja üle;
5) haldab mitut teenuseosutajat mõjutavat turvahaavatavust;
6) tagab, et teatatud turvahaavatavusega seoses võetakse hoolikalt järelmeetmeid;
7) tagab potentsiaalsest turvahaavatavusest või turvahaavatavusest teatava füüsilise või juriidilise isiku anonüümsuse;
8) teeb küberintsidentide käsitlemise riiklike üksuste võrgustikus koostööd teise Euroopa Liidu liikmesriigi poolt turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid täitma määratud küberintsidentide käsitlemise riikliku üksusega, kui teatatud turvahaavatavus võib oluliselt mõjutada teenuseosutajaid rohkem kui ühes Euroopa Liidu liikmesriigis.

(1^4) Ameti peadirektor võib lõike 1 punktis 4 ning lõigetes 1^1 ja 1^3 sätestatud ülesandeid § 15 punkti 2 alusel üle anda teisele struktuuriüksusele, sätestades ülesande vastava struktuuriüksuse põhimääruses.“;

7) määrust täiendatakse normitehnilise märkusega järgmises sõnastuses:

„Euroopa Parlamendi ja nõukogu direktiiv (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).“.

(allkirjastatud digitaalselt)

Liisa-Ly Pakosta
justiits- ja digiminister

(allkirjastatud digitaalselt)

Tiina Uudeberg
kantsler