26.05.2023

Majandus- ja infotehnoloogiaministri määruse „Küberintsidentide registri põhimäärus“ eelnõu seletuskiri

1. Sissejuhatus

1.1. Sisukokkuvõte

Määruse eelnõu kohaselt asutatakse riigi infosüsteemi mitte kuuluv andmekogu ametliku nimetusega küberintsidentide register (edaspidi ka *register*) ning kehtestatakse selle pidamise põhimõtted.

Määrus kehtestatakse küberturvalisuse seaduse (edaspidi *KüTS)* § 13 lõike 3 alusel.

KüTS § 13 kohaselt on küberintsidentide register Riigi Infosüsteemi Ameti peetav andmekogu, kuhu kantakse küberintsidenti kirjeldavad andmed eesmärgiga pidada küberintsidentide üle arvestust nende tuvastamiseks, analüüsimiseks, lahendamiseks, ohuteadete edastamiseks ja järelevalve teostamiseks. Küberintsidentide register koondab endas informatiivset teavet Eesti arvutivõrkudes toimuvate ja Riigi Infosüsteemi Ametile edastatud või Riigi Infosüsteemi Ameti poolt võrgu- ja infosüsteemides tuvastatud küberintsidentide kohta, sh ka teistest eriseaduste alusel Riigi Infosüsteemi Ametile tehtavaid teavitusi[1].

1.2. Ettevalmistajad

Ettepaneku määruse eelnõu ja seletuskirja koostamiseks esitas Riigi Infosüsteemi Ameti õigusnõunik Silver Lusti (silver.lusti@ria.ee). Eelnõu valmistas ette Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse õigusnõunik Guido Pääsuke (guido.paasuke@mkm.ee). Eelnõule tegi õiguslikke ettepanekuid Majandus- ja Kommunikatsiooniministeeriumi õigusosakonna õigusnõunik Ave Henberg (ave.henberg@mkm.ee). Eelnõu on keeleliselt toimetanud Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse õigusnõunik Raavo Palu (raavo.palu@mkm.ee).

Eelnõu ei ole seotud muu menetluses oleva eelnõuga. Eelnõu saadetakse kooskõlastamisele teistkordselt, eelmise kooskõlastuse toimik eelnõude infosüsteemis on 21-0078.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb 14-st paragrahvist, mis jaotuvad nelja peatüki vahel

Eelnõu 1. peatükis on üldsätted.

Paragrahvis 1 nähakse ette andmekogu asutamine. Registri nimetus on vastavalt KüTS §-le 13 küberintsidentide register.

[1] Näiteks E-identimise ja e-tehingute usaldusteenuste seaduse (edaspidi *EUTS*) § 4 kohased teated turvaintsidentidest ja elektroonilise side seaduse (edaspidi *ESS*) §87² lõike 2 kohased teavitused sidevõrgu ja –teenuse turvalisuse ning terviklikkuse tagamist ohustavatest juhtumitest.

Paragrahvis 2 tuuakse välja registri pidamise eesmärk. Registri pidamisel ja andmete töötlemisel lähtutakse avaliku teabe seaduse (edaspidi *AvTS*) §-s 43^1 ja KüTS §-s 13 sätestatud eesmärgist, mille kohaselt on küberintsidentide registri puhul tegemist Riigi Infosüsteemi Ameti peetava ja infosüsteemis töödeldava korrastatud andmete kogumiga, kuhu kantakse küberintsidenti kirjeldavad andmed, eesmärgiga pidada küberintsidentide üle arvestust ning analüüsida neid nende lahendamiseks, ohuteadete edastamiseks ja järelevalvetoimingute läbiviimise toetamiseks. Küberintsident käesoleva põhimääruse mõistes on vastavalt KüTS § 2 punktile 3 võrgu- ja infosüsteemis toimuv sündmus, mis ohustab või kahjustab võrgu- ja infosüsteemi turvalisust.

Registri pidamine aitab kaasa näiteks uute küberintsidentide tuvastamisele, kui registrisse on kantud ründevektorid või muud indikaatorid pahavara liigi või metoodika osas, kuivõrd võimaldab tuvastada samalaadseid olukordi ka muudes võrgu- ja infosüsteemides.

Lahendamisele aitab kaasa registrisse kogutud teave võrgu- ja infosüsteemide nõrkuste kohta, sh näiteks kuidas nõrkuseid kõrvaldada. Sellise teabe kogumine võimaldab seda jagada ka teistega, et nõrkuste kõrvaldamine oleks kiire ja efektiivne. Teabe jagamise all peetakse silmas KüTS § 12 lõike 3 kohaseid ohuteateid. Ohuteated on tuvastatud intsidentide analüüsi tulemusena valminud isikustamata kujul esitatavad juhised näiteks ohtudest või levinud nõrkustest ja lahendustest nende nõrkuste kõrvaldamiseks.

Paragrahvis 3 sätestatakse registri vastutav töötleja ehk registripidaja, kelleks on Riigi Infosüsteemi Amet. Vastavalt AvTS § 43^4 lõikele 1 korraldab vastutav töötleja andmekogu kasutusele võtmist ja andmete haldamist ning vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest. KüTS § 13 lõike 1 kohaselt on tegemist Riigi Infosüsteemi Ameti peetava andmekoguga. Andmekogu kasutatakse üksnes organisatsiooni sisemise töökorralduse vajadusteks oma avalike ülesannete täitmiseks ehk tegemist on riigi infosüsteemi mittekuuluva andmekoguga ja andmevahetuskihiga seda ei liideta. Riigi Infosüsteemi Amet majutab küberintsidentide registrit ise ning korraldab registri teenuste ja tehnoloogilise keskkonna haldamise. Registril ei ole volitatud töötlejaid.

Paragrahvis 4 kohaselt on andmekogusse kantud andmetel informatiivne tähendus.

Paragrahvis 5 tuuakse välja, et tegemist on ühetasandilise digitaalse registriga. Andmed töödeldakse nii automatiseeritult kui ka automatiseerimata.

Paragrahvis 6 sätestatakse registri turvaklass ja turbeaste. Registri turvaklass ja turbeaste on määratud vastavalt Vabariigi Valitsuse 09. detsembri 2022. a määrusele nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded". Turvaosaklassid on määratud järgnevalt: (i) andmete käideldavuse alusel K1, kuivõrd töökindlus peab olema tagatud vähemalt 90% ulatuses. Registri käideldavuse kadu ka rohkem kui 10% olulisel määral asutuse funktsioonide täitmist ei mõjuta. Häiritud oleks näiteks ennetustöö tarbeks analüüside tegemine; (ii) terviklikkuse alusel T1, kuivõrd info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad ning info õigsuse, täielikkuse ja ajakohasuse kontroll erijuhtudel ning vastavalt vajadusele; (iii) konfidentsiaalsuse alusel S2, info asutusesiseseks kasutamiseks, info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele ja juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmisvajaduse korral. Lähtuvalt KüTS § 12 lõikest 5 sisaldab register muuhulgas andmeid ettevõtete ärisaladuse kohta ja Riigi Infosüsteemi Amet on kohustatud seda teavet kaitsma kolmandate isikute eest. Registri turbeaste on seetõttu määratud vastavalt

Vabariigi Valitsuse 09. detsembri 2022. a määrusele nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded" § 8 lõikele 2 keskmine (M).

Registri turbeaste on määratud lähtuvalt asjaolust, et register on üksnes asutusesiseseks kasutamiseks mõeldud. Registri käideldavuse probleemide korral on võimalik talletada sissetulevat teave küberintsidentide kohta ajutiselt alternatiivsetes kanalites (nt dokumendihaldussüsteem) ning teabe vahetus, sh ohuteadete edastamine jt asutuse funktsioonid, sellest ei sõltu.

Eelnõu 2. peatükis on reguleeritud andmete koosseis ja andmete esitamine registrisse.

Paragrahv 7 lõige 1 sätestab milliseid andmeid registrisse kantakse küberintsidendi kohta. Küberintsidendi teada saamisel võib esineda olukordi, kus küberintsidendiga seotud teave ei ole kohe või terviklikult kättesaadav, seetõttu võib küberintsidendist teada saamisel vastutav töötleja kanda registrisse küberintsidenti puudutava teabe osaliselt.

Registrisse kantakse küberintsidendi kohta järgmised andmed:
1) küberintsidendist mõjutatud võrgu- ja infosüsteemi haldaja nimi;
2) intsidendi mõju ulatus;
3) intsidendi avastamise, eeldatava tekkimise ja lahendamise aeg;
4) loetelu võrgu- ja infosüsteemidest, mida küberintsident mõjutab või võib mõjutada;
5) intsidendi tekkepõhjuse kirjeldus;
6) intsidendist teavitanud isik (andmeandja) ja intsidenti lahendav isik (lahendaja);
7) intsidendi lahendamiseks kulunud aeg ja rakendatud turvameetmete kirjeldus;
8) intsidendi tuvastamiseks, analüüsimiseks ning lahendamiseks edastatud lingid, failid ja logid.

Ülalnimetatud teave on vajalik, et hinnata küberintsidendist tulenevat ohtu ja selle lahendamist. Tegemist on ühe küberintsidendiga seotud võimalikest andmetest, mis aitavad kaasa reageerimisele ning lahendamisele. Loetelus olevat teavet tuleb vaadata võimalikult avaralt ehk näiteks mõju ulatuse all peetakse silmas muuhulgas ka piiriülese mõju olemasolu. Samas ei ole kõigi loetelus olevate andmeväljade täitmine kohustuslik, kuna alati ei pruugi küberintsidendi kohta olla iga loetelus oleva punkti kohta teavet ning see teave ei pruugi igal üksikul juhul olla vajalik registri eesmärgi täitmiseks. Samas on kogutav teave vajalik küberintsidendi lahendamiseks Riigi Infosüsteemi Ameti poolt või ka intsidendist täpsema teabe saamiseks, sündmustest ülevaate saamiseks ning vajadusel ka ennetusmeetmete planeerimiseks. Küberintsidendist mõjutatud võrgu- ja infosüsteemi haldaja andmetena käsitletakse võrgu- ja infosüsteemi haldava (sh omanik) juriidilise isiku või füüsilise isiku nime.

Lõikes 2. täpsustakse millist teavet kogutakse küberintsidendi teavitaja ja lahendaja kohta. Küberintsidendid puudutavad erinevaid võrgu- ja infosüsteeme, siis eelduslikult on küberintsidendist teavitaja juriidiline isik. Juriidilise isiku all mõeldakse ka esinevaid riigi- ja kohaliku omavalitsuse asutusi. Selleks, et vajadusel saada lisaks küberintsidendist teavitusele esitatule teavet küberintsidentist endast või selle lahendamisest, kantakse registrisse ka teave küberintsidenti lahendava juriidilise isiku kontaktisiku kohta (ees- ja perenimi ning kontaktandmed (nt telefoninumber ja e-postiaadress)) Küberintsidendist teavitaja võib olla ka rahvusvaheline organisatsioon või välisriigi asjaomane ametiasutus või ka välisriigis tegutsev juriidiline isik (nt Meta Platforms Inc.)

Lisaks küberintsidendist teavitaja andmetele kantakse registrisse ka teave küberintsidendi lahendaja kohta. Lahendav asutus/isik ei pruugi olla sama, mis teavitanud asutus/isik, mistõttu

on vajalik ka nende eristamine. Sarnaselt teavitusele kantakse registrisse ka lahendava juriidilise isiku esindaja andmed, kellega saab vajadusel võtta kontakti.

Kolmandana kantakse registrisse ka teave füüsiliste isikute kohta, kes võivad vabatahtlikult esitada teavitusi küberintsidentidest. Ka nende puhul kantakse registrisse ees- ja perenimi ning kontaktaadress. Füüsiliste isikute poolt laekub teavet näiteks õngitsuskirjade kohta või siis ka võimalike arvutiviiruse kohta või vihjeid võrgu- ja infosüsteemide turvaaukude kohta.

Paragrahvis 8 sätestatakse küberintsidentide kohta vastutavale töötlejale teavet esitavate isikute ehk andmeandjate ring. Andmeandjateks ehk küberintsidendist teatajaks on teenuse osutaja KüTS-i § 3 lõike 1 tähenduses ehk isik, kes kasutab võrgu- ja infosüsteemi järgmiselt:
1) hädaolukorra seaduses sätestatud elutähtsa teenuse osutaja elutähtsa teenuse osutamisel;
2) raudteeseaduses sätestatud raudtee-ettevõtja, kes majandab avalikku raudteeinfrastruktuuri või kelle kaubaveo või reisijateveo turuosa on vähemalt 20 protsenti kaubaveo või reisijateveo turuosast avaliku raudtee toimimise ning raudteeveo ja avaliku reisijateveo toimimise teenuse osutamisel;
3) lennundusseaduses sätestatud lennuvälja käitaja, kelle käitatav lennuväli on avatud rahvusvaheliseks regulaarseks lennuliikluseks, samuti Tallinna lennuinfopiirkonnas lennuliikluse teenindamist tagav aeronavigatsiooniteenuse osutaja lennuvälja toimimise ja aeronavigatsiooni toimimise teenuse osutamisel;
4) sadamateenuse osutaja, kes on sadamaseaduse tähenduses sellise sadama pidaja või sellise sadamarajatise valdaja, mis teenindab 500-se ja enama kogumahutavusega laevu või rahvusvahelises meresõidus sõitvaid reisilaevu sadama toimimise teenuse osutamisel;
5) elektroonilise side seaduses sätestatud sideettevõtja, kes osutab kaabelleviteenust, mida tarbib vähemalt 10 000 lõppkasutajat, ja ringhäälinguvõrgu teenuse osutaja kaabelleviteenuse või ringhäälinguvõrgu teenuse osutamisel;
6) tervishoiuteenuste korraldamise seaduses sätestatud haiglavõrku kuuluvate piirkondliku haigla ja keskhaigla pidaja statsionaarse eriarstiabi osutamisel ja kiirabibrigaadi pidaja kiirabi osutamisel;
7) tervishoiuteenuste korraldamise seaduses sätestatud perearst üldarstiabi osutamisel;
8) Eesti maatunnusega seotud tipptaseme domeeninimede registri haldaja registri pidamiseks kasutatava süsteemi ja tipptaseme nimeserveri teenuse osutamisel;
9) kriitilise tähtsusega side-, mereraadioside ja operatiivraadiosidevõrgu teenuse osutaja elektroonilise side seaduse tähenduses nende teenuste osutamisel;
10) Eesti Rahvusringhääling Eesti Rahvusringhäälingu seaduse § 5 lõike 1 punktis 10 sätestatud ülesande täitmisel.

Lisaks eeltoodud teenustele kogutakse andmeid või osutatakse küberkeskkonnas avalikke teenuseid ka riigi- ja kohaliku omavalitsuse üksuste poolt. Ka sellised avalikud teenused on võimalike küberrünnete sihtmärgid, kui ründaja eesmärgiks on saada näiteks teavet avaliku sektori toimimisest või saada enda valdusesse asutusele avaldatud isikuandmeid, mistõttu KüTS § 3 lõike 4 kohaselt kohaldatakse ka osadele avaliku sektori asutustele KüTSis teenuse osutaja kohta sätestatut. Sellest tulenevalt on küberintsidendist teavitamise kohustus:
1) (riigi- või kohaliku omavalitsuse) andmekogu vastutava töötlejal ja volitatud töötlejal;
2) Arenguseire Keskusel;
3) Eesti Pangal;
4) kohaliku omavalitsuse üksusel ja kohaliku omavalitsuse üksuste liidul;
5) kohtuasutusel;
6) riigi valimisteenistusel;
7) Riigikogu Kantseleil;

8) Riigikontrollil;
9) Riigimetsa Majandamise Keskusel;
10) seaduse alusel asutatud avalik-õiguslikule juriidilisele isikul;
11) Vabariigi Presidendi Kantseleil;
12) valitsusasutusele ja valitsusasutuse hallataval riigiasutusel;
13) valla või linna ametiasutusel, valla või linna ametiasutuse hallataval asutusel, osavallal, linnaosal, osavalla või linnaosa ametiasutusel, osavalla või linnaosa ametiasutuse hallataval asutusel ning kohaliku omavalitsuse üksuste ühisametil ja -asutusel;
14) Õiguskantsleri Kantseleil.

KüTS § 8 lõike 1 kohaselt teavitatakse Riigi Infosüsteemi Ametit viivitamata, kuid hiljemalt 24 tundi pärast teada saamist küberintsidendist:
1) millel on süsteemi turvalisusele või teenuse toimepidevusele oluline mõju;
2) mille oluline mõju süsteemi turvalisusele või teenuse toimepidevusele ei ole ilmne, kuid seda võib mõistlikult eeldada.

KüTS § 8 lõike 4 kohaselt on ettevõtjatel ja asutustel õigus teavitada Riigi Infosüsteemi Ametit küberintsidendist, millel ei ole sätestatud olulist mõju.

Teavituskohustust ei ole KüTS § 1 lõikest 2 tulenevalt, kui küberintsident on seotud:
1) riigisaladuse ja salastatud välisteabe töötlemisele ning sellise teabe töötlussüsteemide pidamisega;
2) Kaitseministeeriumi valitsemisalas rahvusvaheliseks sõjaliseks koostööks ja riigi sõjalise kaitse ettevalmistamiseks vajalike võrgu- ja infosüsteemide pidamisega.

Lisaks kohustuslikule esitamisele KüTS-i tähenduses teenuse osutajate ja avaliku sektori asutuste poolt võib teavitusi küberintsidendist laekuda ka muudelt isikutelt, kellele KüTS-iga ei ole pandud kohustust Riigi Infosüsteemi Ametit teavitada. Muu isiku all peetakse silmas nii tuvastamata kolmandaid isikuid (nt Riigi Infosüsteemi Ametile saadetud e-kiri, mille tegelik esitaja ei ole teada), kui ka E-identimise ja e-tehingute usaldusteenuste seadus tähenduses usaldusteenuse osutajaid ja elektroonilise side seaduse tähenduses sideettevõtjaid, kes ei kuulu KüTS-i teenuse osutajate hulka. Küberintsidendist teatanud isik ei pruugi tingimata olla ise küberintsidendist mõjutatud isik (võrgu- ja infosüsteemi haldaja). Andmeandjaks saab pidada ka Riigi Infosüsteemi Ametit (vastutav töötleja), kui küberintsident on tuvastatud oma avaliku ülesande täitmise raames, näiteks Eesti internetiprotokolli aadressiruumis olevate ning Eesti maatunnusega seotud domeenide vaatlusel ehk kui küberintsidentide ennetamiseks teostatava seire tulemusena tuvastatakse küberintsident. Muu isikuna võib olla käsitletud ka KüTS-i subjekt, kuid kui teavitus puudutab teiste isikute võrgu- ja infosüsteeme, siis ei ole tegemist seadusest tuleneva kohustusega (KüTS subjekti tarneahelas avastatud küberintsident). Näiteks võib esineda olukorda, kus riigiasutus teavitab kahtlusest, et elutähtsa teenuse osutaja võrgu- ja infosüsteem võib olla kahjustatud, või teavitajaks on hoopis rahvusvaheline organisatsioon või välisriigi äriühing.

Paragrahv 9 käsitleb registritoimingute tegemist.
Lõike 1 kohaselt on tehtavateks registritoiminguteks andmete registrisse kandmine, andmete muutmine, andmete vaatamine, andmete edastamine ja andmete kustutamine.

- Andmete registrisse kandmisena mõistetakse küberintsidendi kohta kande avamist registris. Kande avamine toimub kas Riigi Infosüsteemi Ameti enda poolt avastatud küberintsidendi kohta teabe registrisse kandmisega või kui ametini jõuab sama teave

elektroonilisi kanaleid (nt e-postiaadressi cert@cert.ee või veebivormi https://raport.cert.ee/ kaudu) ning selle alusel avatakse kanne. Pärast teavituse alusel kande avamist tehtavad kandega seotud muudatusi käsitletakse andmete muutmisena. Muutmine on nii täiendava teabe lisamine intsidendi kohta või ka siis teabe parandamine.
- Andmete vaatamine on vaid teabe vaatamine ilma sisu muutmata. Vaatamine võib olla ka seotud Riigi Infosüsteemi Ameti vajadusega täita küberturvalisuse seaduses tulenevaid muid ülesandeid.
- Andmete edastamine käib üksnes päringute alusel AvTS § 38 lõigete 3 ja 3^1 kohaselt õigusliku aluse ja eesmärgi kirjelduse esitamisel.
- Kustutamise all mõeldakse küberintsidendi kande lõplikku kustutamist registrist. Küberintsidenti puudutavate ebaõigete andmete kustutamise korral on tegemist andmete muutmisega.

Lõike 2 kohaselt on kõikide toimingute tegemise õigus vastutaval töötlejal, kelleks on Riigi Infosüsteemi Ameti teenistuja, kelle teenistusülesandeks on registri vastutava töötleja ülesande täitmine. Sellisel juhul antakse neile juurdepääs vaid näiteks vaatamiseks. Toimingu tegemise õiguste tase määratakse lähtuvalt tööülesannetest ja teadmisvajadusest, kusjuures õigusi andmekogus toimingute tegemiseks võib määrata kasutajarühmade kaupa või isikupõhiselt.

Lõike 3 ja 4 kohaselt säilitatakse registris registritoimingu kohta toimingu tegija tuvastamist võimaldavad andmed, toimingu tegemise kuupäev ja kellaaeg ning toimingu liik. Täpsem teave, millised registritoimingute andmed säilitatakse, sätestatakse asutusese siseses töökorralduse dokumendis, mis käsitleb muuhulgas registri juurdepääsuõiguste andmise, andmete töötlemise jms põhimõtteid. Kõnealust teavet toimingu kohta säilitatakse üks aasta alates toimingu tegemisest. Töötlemist käsitleva teabe säilitamise peaeesmärk on võimaldada andmete, sh isikuandmete õiguspärase kasutamise kontroll.

Paragrahvis 10 lõikes 1 tuuakse välja, et andmeandjad vastutavad küberintsidentide registrisse esitatud andmete õigsuse eest. Seega kannab vastutav töötleja e-postiaadressile cert@cert.ee edastatud teabe registrisse muutmata kujul

Lõikega 2 antakse vastutavale töötleja õigus küberintsidentide registris andmete ebaõigsuse kindlaks tegemisel nende parandamiseks ehk muutmiseks. Parandamist võib vaja minna näiteks olukorras, kus esmane teavitus täpsustub või saadakse teada uusi asjaolusid küberintsidendi kohta jne.

Eelnõu 3. peatükis sätestatakse registrile juurdepääs ja andmete säilitamine.

Paragrahvis 11 kirjeldatakse andmekogule juurdepääsuõiguse andmist.
Lõige 1. Registriandmed on tunnistatud KüTS § 13 lõike 3 kohaselt asutusesiseseks kasutamiseks ning seetõttu on ka selles olevale teabele piiratud juurdepääs, mis põhineb teadmisvajadusel. Piirangud on kehtestatud eelkõige sellest, et registriandmed võivad sisaldada teavet turvasüsteemide või turvameetmete kirjelduse või tehnoloogiliste lahenduste kohta. Samuti võib registrisse kantud teave sisaldada isikuandmeid või ka KüTS-i tähenduses teenuse osutajate kohta käivat teavet, mida soovitakse kaitsta avalikuks tuleku eest. Olenevalt küberintsidendi asjaoludest võib olla juurdepääsupiirangu seadmine põhjendatud ka muudel alustel kooskõlas avaliku teabe seadusega.

Lõike 2 kohaselt andmetele juurdepääsu registriandmetele Riigi Infosüsteemi Ameti ametnikule ja töötajale oma töö- või teenistusülesannete täitmiseks. Tegemist on Riigi

Infosüsteemi Ameti töötajatega, kelle ülesandeks ei ole või ülesanne ei puuduta registri vastutava töötaja ülesannete täitmist. Juurdepääsu andmine toimub antud juhul eelkõige registrisse sisselogimise teel. Seejuures tuleb vastutaval töötlejal määrata nende isikute kasutajakonto õiguste klass jne.

Lõike 3 kohaselt võib registriandmeid väljastada:

- andmeandjale tema poolt esitatud teabe osas. Tegemist on isiku õigusega saada teavet oma esitatud teabe kohta;
- andmekaitse järelevalveasutusele, kui küberintsident on seotud katsega kätte saada isikuandmeid või küberintsidendi tulemusel on isikuandmed kättesaadavaks saanud selleks mitteõigustatud isikule. Küberintsidendid on sageli seotud sooviga saada enda valdusesse isikuandmeid, sealhulgas eriliigilisi isikuandmeid. Sellest tulenevalt on ennetusetegevuse ja järelevalve teostamiseks vajalik andmekaitseasutuste teavitamine. Eestis näiteks on vajalik Andmekaitse Inspektsiooni teavitamine küberintsidendist, mis on seotud katsega saada oma valdusesse isikuandmeid. Eelnõus esitatud tingimused on välja toodud, et andmete valimatud edastamisega ei koormataks andmekaitseasutust.
- Riigi julgeoleku tagamisega seotud ülesannete täitmiseks. Küberintsident võib olla põhjustatud eesmärgiga saada kätte avalikku teavet või siis teavet Eesti elanike kohta. Olulise mõjuga küberintsident võib põhjustada olulist kahju Eesti riigi julgeolekule ja sõltumatusele, mistõttu on teave vajalik julgeolekuasutustele, et hinnata ohtusid ja nende esinemist ning päritolu;
- süütegude menetlemisel. Küberintsidentide kohta kogutud teave sh ründevektorid, IP-aadressid jms võib olla olulise väärtusega küberkuritegude uurimiseks ja menetlemiseks. Küberintsidendid võivad olla seotud ka muude süütegudega kui vaid võrgu- ja infosüsteemi kahjustamine. Küberintsident võib olla seotud sooviga omandada ebaseaduslikult isikute finantsvara või rahalisi vahendeid, mistõttu võib intsidendi raames saadud teave olla olulise väärtusega süütegude lahendamisel;
- kui see on vajalik suure mõjuga küberintsidendi lahendamiseks ja teabe edastamine on ettenähtud seadusega või rahvusvahelise lepinguga. Eesti teeb koostööd teiste riikide ja organisatsioonidega küberkeskkonna turvalisuse tagamiseks ja suure mõjuga intsidentide ennetamiseks ning tõrjumiseks, mistõttu on vajalik vastastikune teabe vahetus. Teabevahetus Euroopa Liidu liikmesriikide asjaomaste asutustega on ettenähtud ka Euroopa Parlamendi ja Nõukogu 06.07.2016 direktiiviga (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus. Säte arvestab asjaoluga, et küberintsidenti puudutav teave võib olla vajalik välisriigis kübeturvalisuse tagamisega seotud asutusele või Euroopa Liidu Võrgu- ja Infoturbeametile (edaspidi *ENISA*) või muule rahvusvahelisele organisatsioonile (nt EUROPOL);
- lisaks eeltoodud peamistele võimalikele teabe tarbijatele võib esineda muid olukordi, kus küberintsidendiga seotud teave on seotud avalik ülesande täitmisega. Eelkõige on need valdkonnad seotud ohtude ennetamisega, korrakaitsega või õiguse mõistmisega. Nii näiteks ei saa välistada, et registris olev teave on vajalik kohtumenetluse raames ning kohus nõuab teabe välja. Või Finantsinspektsioon soovib oma menetluse raames teavet hindamaks, kas finantsasutus on käitunud korrektselt sündmuste lahendamisel või Riigikantselei vajab teavet üldise ohuennetuse raames. Lisaks arvestab säte, et Euroopa Liidu ja Eesti tasemel on menetluses õigusaktide eelnõud, millega laiendatakse kübervaldkonnas saadud teabe kasutamist üldiste ja avalike huvide kaitsemisel.

Lõike 4 sätestatakse vastutava töötleja õigused registriandmete väljastamisel. Registriandmetele juurdepääsu saamiseks peab isik esitama põhistatud taotluse, millele

vastamiseks on vastutaval töötlejal aega 30 päeva. Vastutaval töötlejal on õigus ka küsida lisateavet veendumaks isiku õiguses kasutada registriandmeid, sealhulgas teadmisvajaduses. Isiku enda esitatud andmete korral teadmisvajadust ei kontrollita.

Lõikes 5 sätestatakse õigus väljastada registri andmed ka omal algatusel, kui selline kohustus on sätestatud seadusega või rahvusvahelise lepinguga. Näiteks ENISA teavitamine piiriülese mõjuga küberintsidendist KüTS § 12 lõike 4 alusel, eeldusel, et teabe edastamine ei kahjusta riigi julgeolekut või kriminaalmenetlust.

Lõikes 6 sätestatakse vastutava töötleja kohustus pidada arvestust registrist väljastatud andmete üle, säilitades andmed kellele, millisel eesmärgil, millal, millisel viisil ja missuguseid andmeid registrist väljastatakse. Lõikes sätestatud arvepidamist võib teha näiteks dokumendihalduse süsteemi kasutades. Registriandmete väljastamise täpsema arvestuse võib Riigi Infosüsteemi Amet kehtestada oma sisemiste juhistega.

Paragrahvi 12 lõige 1 määrab andmete säilitamise tähtajaks viis aastat alates küberintsidendi lahendamisest. Küberintsidendi lahendamiseks loetakse küberintsidentide registris vastutava töötleja poolt vastava kande tegemist, millega loetakse juhtum lõpetatuks. Olulise mõjuta küberintsidendi korral, kui võrgu- ja infosüsteemi käideldavusele, terviklusele või konfidentsiaalsusele ei ole avaldunud mõju, võib küberintsidendi märkida lahendatuks juba selle registrisse kandmisel. Näiteks on selliseks teateks teavitused õngitsuskirjadest, mille ohvriks ei ole teadaolevalt keegi langenud.

Viie aastane säilitamise tähtaeg on oluline, et näha muu hulgas ajas muutuvaid trende ja ründevormide arenguid, sh loomaks seoseid ajaliselt hiljem tehtud analüüside tulemite ja ajas varasemalt aset leidnud intsidentide vahel. Viis aastat on piisavalt pikk aeg, et olulisemad seosed võiksid välja tulla ning sellest teabest lähtuvalt saab anda täiendavaid ohuhinnanguid või teha ohuteateid. Teabe esitanud isiku andmete säilitamisel on arvestatud vajadust saada isikult täiendavat teavet sündmuse kohta, kui sündmuse juures tuvastatakse pikaajaline seos või mingi muu oluline asjaolu, mis võimaldab sündmust või intsidendi eesmärki paremini mõista. Lõike 2 kohaselt pärast säilitustähtaja saabumist andmeid ei arhiveerita vaid kustutatakse registrist. Võib tekkida olukord, kus kustutatud teabe osas säilivad registri väliselt mingit teavet. Näiteks registri andmete alusel tehtud isikustamata ülevaated ja analüüsid, mida töödeldakse (sh säilitatakse ja kasutatakse) edasi.

Eelnõu 4. peatükis on reguleeritud registri rahastamine ja likvideerimine.

Paragrahv 13 kohaselt rahastatakse registri pidamist, sh arendus- ja hooldustöid riigieelarvest Riigi Infosüsteemi Ametile eraldatud eelarvevahenditest. Osaliselt on registri arendus- ja hooldustöödeks kaasatud struktuurifondide (SF) või Euroopa ühendamise (CEF) rahastust, kuid see ei ole mõeldud registri pideva toimimise tagamiseks.

Paragrahvis 14 sätestatu kohaselt otsustab küberintsidentide registri likvideerimise valdkonna eest vastutav minister. Likvideerimisel tuleb otsustada andmete teise andmekogusse või avalikku arhiivi üleandmine või andmete hävitamine või nende üleandmine vastavalt arhiiviseaduses või selle alusel antud õigusaktide sätestatule..

Seadusest tulenevalt teostab registri pidamise üle järelevalvet Andmekaitse Inspektsioon, mistõttu seda määruses ei korrata.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu on vastavuses Euroopa Liidu õigusega. Eelnõu on kooskõlas Euroopa Parlamendi ja Nõukogu 06.07.2016 direktiiviga (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus, mille kohaselt liikmesriigid tagavad asjaomase asutuste teavitamise küberintsidentidest nii liikmesriigi siseselt kui ka liikmesriikide üleselt. Samuti on eelnõu seotud vajadusega luua asjakohane teavitussüsteem ning tagada vajalik teabevahetus. Teabevahetus peab tagama asjaomase teabe konfidentsiaalsuse ning asjakohaste meetmete rakendamise oluliste teenuste operaatorite ja digitaalse teenuse osutajate turvalisuse ja ärihuvide kaitse registrisse teabe edastamisel.

4. Määruse mõjud

Määruse rakendamisega ei kaasne otsest sotsiaalset ja demograafilist mõju, ega mõju välissuhetele, majandusele ega mõju elu- ja looduskeskkonnale, regionaalarengule, riigiasutuste ning kohaliku omavalitsuse korraldusele ega muud otsest ja kaudset mõju. Määrusega seotud mõjud on toodud XIV Riigikogu menetluses olnud küberturvalisuse seaduse 597 SE juures. Eelnõu rakendamisega võib ette näha mõju riigiasutuste ja kohaliku omavalitsuse korraldusele, täpsemalt Riigi Infosüsteemi Ametile.

Kaasnev mõju: mõju riigiasutuste ja kohaliku omavalitsusese korraldusele
Sihtrühm: Riigi Infosüsteemi Amet
Mõju ulatus: Määruse jõustumisel on võimalik Riigi Infosüsteemi Ametil süstematiseerida küberintsidentide teavitused ja nende lahendamised. Korrastatud ülevaate tulemusel on võimalik tõhustada ennetamist ja koordineerida või juhendada küberintsidentide lahendamist ning anda soovitusi sündmustele reageerimiseks. Määrus mõjutab Riigi Infosüsteemi Ameti ülesannete täitmist positiivselt ning võimaldab Riigi Infosüsteemi Ametil kiiremini reageerida ohtudele ning analüüsida ja efektiivsemalt tagasisidestada võrgu- ja infosüsteemide kaitsega seonduvat.

5. Määruse rakendamisega seotud tegevused, vajalikud kulud ja määruse rakendamise eeldatavad tulud

Määruse rakendamine ei too riigieelarvele kaasa täiendavat kulu ega tulu. Määruse rakendamisega kaasnev kulu kaetakse iga-aastaselt riigieelarvest Riigi Infosüsteemi Ametile eraldatud riigieelarveliste vahendite arvelt.

6. Määruse jõustumine

Määrus jõustub üldises korras ehk kolmandal päeval pärast Riigi Teatajas avaldamist.

7. Määruse eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Määruse eelmine versioon käis avalikul konsultatsioonil 2021. aasta alguses eelnõude infosüsteemi vahendusel (toimik nr 21-0078). Saadud tagasiside ja vastused tagasisidele on leitav seletuskirja lisast.

Määruse eelnõu saadetakse eelnõude infosüsteemi kaudu täiendavaks kooskõlastamiseks ministeeriumitele, Riigikantseleile ning Eesti Linnade ja Valdade Liidule. Eelnõu saadetakse

arvamuse andmiseks Riigi Infosüsteemi Ametile, Andmekaitse Inspektsioonile, Statistikaametile ning Infotehnoloogia ja Telekommunikatsiooni Liidule.